LAW REFORM
COMMISSION/COIMISIÚN UM
ATHCHÓIRIÚ AN DLÍ

CONSULTATION PAPER

DOCUMENTARY AND ELECTRONIC EVIDENCE

(LRC CP 57 - 2009)

FIRST PUBLISHED
December 2009

ISSN 1393-3140

LAW REFORM COMMISSION'S ROLE

The Law Reform Commission is an independent statutory body established by the *Law Reform Commission Act 1975.* The Commission's principal role is to keep the law under review and to make proposals for reform, in particular by recommending the enactment of legislation to clarify and modernise the law. Since it was established, the Commission has published over 150 documents containing proposals for law reform and these are all available at www.lawreform.ie. Most of these proposals have led to reforming legislation.

The Commission's role is carried out primarily under a Programme of Law Reform. Its *Third Programme of Law Reform 2008-2014* was prepared by the Commission following broad consultation and discussion. In accordance with the 1975 Act, it was approved by the Government in December 2007 and placed before both Houses of the Oireachtas. The Commission also works on specific matters referred to it by the Attorney General under the 1975 Act. Since 2006, the Commission's role includes two other areas of activity, Statute Law Restatement and the Legislation Directory.

Statute Law Restatement involves the administrative consolidation of all amendments to an Act into a single text, making legislation more accessible. Under the *Statute Law (Restatement) Act 2002,* where this text is certified by the Attorney General it can be relied on as evidence of the law in question. The Legislation Directory - previously called the Chronological Tables of the Statutes - is a searchable annotated guide to legislative changes. After the Commission took over responsibility for this important resource, it decided to change the name to Legislation Directory to indicate its function more clearly.

MEMBERSHIP

The Law Reform Commission consists of a President, one full-time Commissioner and three part-time Commissioners.

The Commissioners at present are:

President:
The Hon Mrs Justice Catherine McGuinness
Former Judge of the Supreme Court

Full-time Commissioner:
Patricia T. Rickard-Clarke, Solicitor

Part-time Commissioner:
Professor Finbarr McAuley

Part-time Commissioner:
Marian Shanley, Solicitor

Part-time Commissioner:
Donal O'Donnell, Senior Counsel

LAW REFORM RESEARCH STAFF

Director of Research:
Raymond Byrne BCL, LLM (NUI)
Barrister-at-Law

Legal Researchers:
Chris Campbell, B Corp Law, LLB Diop Sa Gh (NUI)
Siobhan Drislane BCL, LLM (NUI)
Gemma Ní Chaoimh BCL, LLM (NUI)
Bríd Nic Suibhne BA, LLB (NUI), LLM (TCD), Diop sa Gh (NUI)
Jane O'Grady BCL, LLB (NUI), LPC (College of Law)
Gerard Sadlier BCL (NUI)
Joseph Spooner BCL (Law with French Law) (NUI), BCL (Oxon) Dip. Fr and Eur Law (Paris II)
Ciara Staunton BCL, LLM (NUI), Diop sa Gh (NUI)

STATUTE LAW RESTATEMENT

Project Manager for Restatement:
Alma Clissmann, BA (Mod), LLB, Dip Eur Law (Bruges), Solicitor

Legal Researchers:
John P Byrne BCL, LLM, PhD (NUI), Barrister-at-Law
Catriona Moloney BCL (NUI), LLM (Public Law)

LEGISLAT ION DIRECTORY

Project Manager for Legislation Directory:
Heather Mahon LLB (ling. Ger.), M.Litt, Barrister-at-Law

Legal Researchers:
Margaret Devaney LLB, LLM (TCD)
Rachel Kemp BCL (Law and German), LLM (NUI)

ADMINISTRATION STAFF

Head of Administration and Development:
Brian Glynn

Executive Officers:
Deirdre Bell
Simon Fallon
Darina Moran
Peter Trainor

Legal Information Manager:
Conor Kennedy BA, H Dip LIS

Cataloguer:
Eithne Boland BA (Hons), HDip Ed, HDip LIS

Clerical Officers:
Ann Browne
Ann Byrne
Liam Dargan
Sabrina Kelly

PRINCIPAL LEGAL RESEARCHER FOR THIS CONSULTATAION PAPER

Gemma Ní Chaoimh BCL, LLM (NUI)

CONTACT DETAILS

Further information can be obtained from:

Head of Administration and Development
Law Reform Commission
35-39 Shelbourne Road
Ballsbridge
Dublin 4

Telephone:
+353 1 637 7600

Fax:
+353 1 637 7601

Email:
info@lawreform.ie

Website:
www.lawreform.ie

ACKNOWLEDGEMENTS

The Commission would like to thank the following people who provided valuable assistance, and a number of whom attended the Commission's roundtable discussions on the projects on hearsay and documentary evidence on 3 and 4 March 2009:

Mr Jevon Alcock, Chief State Solicitors Office
Mr Senan Allen, Senior Counsel
Mr Patrick Brehony, Detective Chief Superintendent, Garda Bureau of Fraud
Ms Rebecca Coen, Office of the Director of Public Prosecutions
Mr Paul Coffey, Senior Counsel
Ms Caroline Costello, Barrister-at-Law
Mr Donogh Crowley, Arthur Cox Solicitors
Ms Valerie Fallon, Dept of Justice, Equality and Law Reform
Mr Remy Farrell, Barrister-at-Law
Mr Michael Finucane, Michael Finucane Solicitors
Mr Eugene Gallagher, Detective Superintendent, Garda Bureau of Fraud
Ms Mary Rose Gearty, Senior Counsel
Mr James Hamilton, Director of Public Prosecutions
Ms Áine Hynes, St John Solicitors
Ms Claire Loftus, Chief Prosecution Solicitor, Office of the Director of Public Prosecutions
Mr Dominic McGinn, Barrister-at-Law
Mr James McMahon, St John Solicitors
Commissioner Fachtna Murphy, Garda Commissioner
Mr Kerida Naidoo, Barrister-at-Law
Mr Lúan O'Braonáin, Senior Counsel
Mr Tadgh O'Leary, CMOD, Department of Finance
Mr Anthony Sammon, Senior Counsel

Full responsibility for this publication lies, however, with the Commission.

TABLE OF CONTENTS

Criminal Justice Act 1994	No. 15/1994	Irl
Criminal Justice Act 2003	2003 c.44	Eng
Documentary Evidence Act 1868	31 & 32 Vict., c. 37	Eng
Documentary Evidence Act 1882	45 & 46 Vict., c. 9	Eng
Documentary Evidence Act 1895	1895 c. 9	Eng
Documentary Evidence Act 1925	No. 24/1925	Irl
Electronic Commerce Act 2000	No. 27/2000	Irl
Electronic Communications Act 2000	2000, c. 7	Eng
Electronic Signatures in Global and National Commerce Act 2000	15 U.S.C. 7001	US
Electronic Transactions Act (Victoria) 2000	No. 20/2000	Vict
Electronic Transactions Act 1999	1999:26	BM
Electronic Transactions Act 1999	No. 162/1999	Aust
Electronic Transactions Act 2002	No. 35/2002	NZ
Evidence (Colonial Statutes) Act 1907	1907 c. 16	Eng
Evidence (Document Unavailability) Act 2006	No. 53/2006	Aust
Evidence Act 1845	8 & 9 Vict., c. 113	Eng
Evidence Act 1851	14 & 15 Vict., c. 99	Eng
Evidence Act 1935	1938 c. 28	Eng
Evidence Act 1995	No. 58/1995	Aust
Evidence Act 1997	No. 76/1977	Qld
Evidence Act 2006	No. 69/2006	NZ
Evidence Act 2008	No. 47/2008	Aust
Finance Act 1983	No. 15/1983	Irl
Insolvency Act 1986	1986 c. 45	Eng
Interception of Postal Packets and Telecommunication Messages (Regulation) Act 1993	No. 10/1993	Irl

Interpretation Act 1978	1978 c. 30	Eng
Interpretation Act 2005	No. 23/2005	Irl
Investment Funds, Companies and Miscellaneous Provisions Act 2006	No. 41/2006	Irl
Land and Conveyancing Law Reform Act 2009	No. 28/2009	Irl
Law of Evidence Amendment Act 1988	No. 45 of 1988	SA
Magistrate's Court Act 1980	1980 c. 43	Eng
Malaysian Digital Signature Act No. 562 of 1997	No. 562/1997	MA
Medical Practitioners Act 1978	No. 4/1978	Irl
National Standards Authority of Ireland Act 1996	No. 28/1996	Irl
New Brunswick Evidence Act on Electronically Stored Documents 1996	SNB 1996 c. 52	CA
Perjury Act 1911	1911 c. 6	Eng
Personal Information Protection and Electronic Document Act 2000	2000 c. 5	CA
Pharmacy Act 2007	No. 20/2007	Irl
Postal and Telecommunications Services (Amendment) Act 1999	No. 5/1999	Irl
Public Records Act 1958 (Admissibility of Electronic Copies of Public Records) Order 2001	S.I. No.4058/2001	Eng
Registration of Birth and Deaths (Ireland) Act 1863	26 & 27 Vict, c. 90	Eng
Road Traffic (Amendment) Act 1978	No. 19/1978	Irl
Road Traffic Act 1994	No. 7/1994	Irl
Rules of the Superior Courts (No. 2) 1993	SI No. 265/1993	Irl
Rules of the Superior Courts (Proof of Foreign, Diplomatic, Consular and Public Documents) 1999	SI No. 3 1999	Irl
Safety, Health and Welfare at Work Act 2005	No. 10/2005	Irl
Social Welfare (Miscellaneous Provisions) Act 2002	No. 8/2002	Irl
Statute Law Revision Act 2007	2007, No 28	Irl
Statute of Frauds (Ireland) 1695	1695, c. 12	Irl

Statute of Frauds 1677	1677, c. 3	Eng
Statutory Declarations Act 1938	No. 37/1938	Irl
Terms of Employment (Information) Act 1994	No. 25/1994	Irl
Terrorism Act 2000	2000 c. 11	Eng
Utah Digital Signature Act 1995	46-3-101	US
Vendor and Purchaser Act 1874	37 & 38 Vict. c. 78	Eng

Bishop Meath v Marquess of Winchester	(1836) 3 Bing NC 183	Eng
Borges v Fitness to Practice Committee of the Medical Council and the Medical Council	[2004] 1 IR 103	Irl
Branagan v Director of Public Prosecutions	[2000] RTR 235	Eng
British American Tabacco Australian Services v McCabe	[2002] VSC 73	Aust
British American Tobacco Australia Services Ltd v Cowell	[2002] VSCA 197	Aust
Brown v Donegal County Council	[1980] IR 132	Irl
Butera v DPP for the State of Victoria	(1987) 146 CLR	Aust
Case No. 19 U 16/02, Oberlandesgericht Koln	September 6, 2002	Ger
Casey v Intercontinental Bank	[1979] IR 364	Irl
Castle v Cross	[1984] 1 WLR 1372	Eng
Caton v Caton	(1867) LR 2 HL 127	Eng
Celotex Corp v Catrett	477 US 317, 106 S Ct. 2548 (1986)	US
Chemical Bank v McCormack	[1983] ILRM 350	Irl
Chestvale Properties v Glackin	[1993] 3 IR 35	Irl
Chicester v Hobbs	(1866) 14 LT 433	Eng
Clifford v Minister for Justice	[2005] IEHC 288	Irl
Clipper Maritime Ltd v Shirlstar Container Transport Ltd (The Anemone)	[1987] 1 Lloyd's Rep 546	Aust
Coleman v Coleman	(1898) 32 ILTR 66	Irl
Commission for Railways (NSW) v Young	(1962) 106 CLR 535	Aust
Compagnie Financiere du Pacifique v Peruvian Guano Co	(1882) 11 QBD 55	Eng

Cooper Flynn v Radio Telefis Eireann	[2000] 3 IR 344	Irl
Crown Life Insurance Co. v Craig	995 F .2d 1376 (7th Cir. 1993)	US
Cunningham v Fair Haven & Westville R. Co.	72 Conn. 244 (1899)	US
Darby v DPP	QBD 4 November 1994,	Eng
Digicel v Cable and Wireless	[2008] EWHC 2522 (Ch)	Eng
Doe d France v Andrews	(1850) 15 QB 756	Eng
Doe d Jacobs v Phillips	(1845) 8 QB 158	Eng
Doe d Mudd v Suckermore	(1837) 5 Al & El 703	Eng
Doe Gilbert v Ross	(1840) 7 M&W 102	Eng
Dome v Telecom Eireann	[2007] IESC 59	Irl
Douglass v Lloyds Bank Ltd	(1929) 34 Com. Cas. 263	Eng
Doust v Schatz	(2002) 227 Sask. R. 1 (CA)	CAN
Dowse v An Bord Uchtala	[2006] IEHC 64	Irl
DPP v McKeown	[1995] Crim LR 69	Eng
Dublin Corporation v Bray Township Commissioners	[1900] 2 IR 88	Irl
Dundalk AFC Interim Co Ltd v FAI National League	[2001] 1 IR 434	Irl
Emmott v Star Newspaper Co.	(1892) 62 LJQB 77	Eng
Evans v Hoare	[1892] 1 QB 593	Eng
Firstpost Homes Ltd v Johnson	[1995] 4 All ER 355	Eng
Fitzpatrick v DPP	[2007] IEHC 383	Irl
Forbes v Samuel	[1913] 3 KB 706	Eng
Framus v CRH Plc	[2004] 2 ILRM 439	Irl
Fyffes Plc v DCC Plc,	High Court, 21 December 2005	Irl
Garton v Hunter	[1969] 1 All ER 451	Eng
Gillespie	(1967) 51 Cr App R 172	Eng
Goodman v Hamilton	[1992] 2 IR 542	Irl

Goodman v J Eban	[1954] 1 QB 550	Eng
Grant v Southwestern and County Properties Ltd	[1975] Ch 185	Eng
Griffiths v Australia and New Zealand Banking Group Limited	(1990) 53 SASR 256	Aust
Hannon v Commissioners of Public Works	. High Court 4 April 2001	Irl
Heyne v Fischel & Co	(1913) TLR 190	Eng
Howard v Beall	(1889) 23 QBD 1	Eng
Hughes v US	953 F .2d (9th Cir. 1992)	US
Hussey v Twomey,[2009] 1 ILRM 321	Irl	
In Re Jahre (Anders)	[1986] Lloyd L Rep 496	Eng
In Re MK, SK and WK, Minors:The Eastern Health Board v MK and Another	[1999] 2 ILRM 321	Irl
In re Vee Vinhnee	336 BR 437 (9th Cir. 2005)	US
JB, O'C v PCD	[1985] IR 265	Irl
Joachimson v Swiss Bank Corporation	[1921] 3 KB 110	ENg
Jones v Jones	(1841) 9 M&W 75	Eng
Jones v Tarleton	9 M & W 675	Eng
Judd v Citibank	435 NYS 2d 210 (1980)	US
Kajala v Noble	(1982) 75 Cr App R 149	Eng
Karmat Auto Spares Pty Ltd v Dominelli Ford (Hurstville) Pty Ltd	(1992) 35 FCR 560	Aust
Kelly v Ross & Ross	High Court, 29 April, 1980	Irl
Kiely v Minister for Social Welfare	[1977] IR 276	Irl
King v State ex rel Murdock Acceptance Corp.	222 So .2d 393 (miss. 1969)	US
L'Aime v Wilson	(1907) 2 IR 130	Irl

Lanigan v Chief Constable	[1991] NI 42	NI
Lewis v Sapio	(1827) Mood & M 39	Eng
Libyan Arab Foreign Bank v Bankers Trust Co.	[1989] QB 728	Eng
Lilley v Pettit	[1946] KB 401	Eng
Lipkin Gorman v Karpnale Ltd	[1992] 4 All ER 409	Eng
Lorraine v Markel American Ins. Co.	241, FRD 534 (D. Md. 2007)	US
Lorraine v Markel American Ins. Co.	241, FRD 534 (D. Md. 2007)	US
Lyell v Kennedy	(1889) App Cas 437	Eng
Markovina v The Queen	(1996) 16 WAR 354	Aust
Martin v Quinn	[1980] IR 244	Irl
Masquerade Music v Springsteen	[2001] EWCA Civ 563	Eng
McCarthy v O'Flynn	[1979] IR 127	Irl
McFarlane v DPP and Another	[2006] IESC 11	Irl
Mehta v J Pereira Fernandes SA	[2006] 2 All ER 891	Eng
Mercer v Dunne	[1905] 2 Ch 538	Eng
Minister for Justice, Equality and Law Reform and the Courts Service v The Information Commissioner	High Court, May 2001	Irl
Minors and Harper	(1989) Cr App R 102	Eng
Monotype Corp. Plc v International Typeface Corp.	43 F. 3d 443 (9th Cir. 1994)	US
Mortimer v M'Callan	(1840) 6 M&W 58	Eng
Mortiner v M'Callan	(1840) 6 M & W 58	Eng
Mulhern v Cleary	[1930] IR 649	Irl
Myres v DPP	[1965] AC 1001	Eng
Nally v Nally	[1953] IR 19	Irl

Narlis v South African Bank of Athens	1976 (2) SA 573, AD	SA
National Irish Bank Ltd v Radio Telefis Eireann	[1998] 2 IR 465	Irl
Nedbank Ltd v Mashiya and Another	2006 (4) SA 422 (T)	Aust
Nikolaidis v Legal Services Commissioner	[2007] NSWSC 130	Aust
NSW Supreme Court, 18 September 1995	Aust	
NT Power Generation Pty Ltd v Power and Water Authority	[1999] FCA 1549	Aust
O'Conghaile v Wallace	[1938] IR 526	Irl
Omychund v Barker	(1745) 1 Atk, 21, 49: 26 ER 15	Eng
Owner v Bee Hive Spinning Co. Ltd	[1914] KB 105	Eng
Palmer v AH Robins Co. Inc.	684 P .2d 187 (Colo. 1984)	US
Parker v Clark	[1960] 1 WLR 286	Eng
Parnell v Wood	[1892] P 137 CA	Eng
People (AG) v Casey (N0. 2)	[1963] IR 33	Irl
People (DPP) v Byrne	[1989] ILRM 613	Irl
People (DPP) v Foley	[2007] 2 IR 486	Irl
People (DPP) v Kavanagh	[2009] IECCA 29	Irl
People (DPP) v Larkin	[2008] IECCA 138	Irl
People (DPP) v Marley	[1985] ILRM 17	Irl
People (DPP) v McCann	Unrep. Central Criminal Court: 31 July 1996	Irl
People (DPP) v McCormack	[1984] IR 177	Irl
People (DPP) v McDermott v Riordan	[2005] IEHC 132	Irl
People (DPP) v Meehan	[2006] 3 IR 468	Irl
People (DPP) v Murphy	[2005] 2 IR 125	Irl

People (DPP) v O'Donoghue	[1991] 1 IR 448	Irl
People (DPP) v O'Reilly	[2009] IECCA 18	Irl
People v Lugashi	252 Cal. Reptr. 434 (Cal. Ct. App. 1988)	US
Porter v Citibank	472 NYS 2d 582 (1984)	US
Post Office Counters v Mahida	[2003] EWEA Civ 1583	Eng
PPS v Duddy	[2008] NICA 18	NI
PPS v McGowan	[2008] NICA 13	NI
Primor Plc v Stokes	[1996] 2 IR 459	Irl
R v Blastand	[1985] 2 All ER 1095	Eng
R v Chen	[1993] 2 VR 149	Aust
R v Clapham	(1829) 4 C & P 29	Eng
R v Clark	[1969] 2 QB 91	Eng
R v Cook (Christopher)	[1987] QB 417	Eng
R v Coventry Magistrates Court	[2004] EWHC 905	Eng
R v Curran and Torney	[1983] 2 VR 133	Aust
R v Dadson	(1983) 77 Cr. App. R 91	Eng
R v Daye	[1908] 2 KB 333	Eng
R v Dhaliwal	(2004) 2 Cr App R 307	Eng
R v Dodson and Williams	[1984] 1 WLR 971	Eng
R v Ensbye; ex parte A-G (QLD)	[2004] QCA 335	Aust
R v Ewing	[1983] QB 1039	Eng
R v Fredericton Housing	[1973] CTC 160 (FCTD)	US
R v Fursey	6 C & P 84	Eng
R v Governor of Brixton Prison and Another, ex p Levin	[1997] 3 WLR 117	Eng
R v Governor of Pentonville ex p Osman	[1989] 3 All ER 701	Eng
R v Halpin	[1975] QB 907	Eng
R v Harper	[1989] 2 All ER 208	Eng

R v Jones	[1978] 1 WLR 195	Eng
R v Kearns	[2002] 1 WLR 2815	Eng
R v Kent Justices	(1874) LR 8 QB 305	Eng
R v Leonard	[2009] EWCA Crim 1251	Eng
R v Maqsud Ali	[1965] 2 All ER 464	Eng
R v Pettigrew	[1980] Crim Law Rep 669	Eng
R v Pitre	[1933] 1 DLR 417	Eng
R v S and Another	[2008] EWCA Crim 2177	Eng
R v Shephard	(1991) 93 Cr App R 139	Eng
R v Smith	[1992] 2 SCR 915	Can
R v South London Coroner ex parte Thompson	(1982) 126 SJ 625	Eng
R v Spiby	(1990) 91 Cr App R 186	Eng
R v Stephens	[1999] 3 NZLR 81	NZ
R v Thompson	[2001] 1 NZLR 129	NZ
R v Wayte	(1982) 76 Cr App R 110	Eng
R v Wiles	(1982) 76 Cr App R 669	Eng
R v Wood	(1982) 76 Cr App R 23	Eng
Rajnowski v Detroit	(1889) BC & ARCo. 41 NW 849	US
Re a Debtor (No. 2021 of 1995)	[1996] 2 All ER 345	Eng
Re Boucher	(2007) WL 4246473	US
Re State of Norway's Application (Nos 1 and 2)	[1989] 1 All ER 745	Eng
Ritz Hotel Ltd v Charles of the Ritz Ltd (Nos 13, 18 and 19)	(1988) 14 NSWLR 116	Aust
Roach v Page (No 15)	[2003] NSWSC 935	Aust
Roe d. West v Davis	(1806) 7 East 363, 103 Eng Rep 140	Eng
RW Miller & Co Pty Ltd v Krupp (Australia) Pty Ltd	(1991) 32 NSWLR 152	Aust
S and Y Investments (No 2) Pty Ltd v Commercial Union	(1986) 82 FLR 130	Aust

Ulster Bank Limited v Byrne	High Court, 10 July 1997	Irl
United States & Fidelity Guaranty Co. v Young Life Campaign, Inc	553 F .2d 1109 (8th Cir. 1976)	US
United States v Bonallo	858 F .2d 1427 (9th Cir. 1988)	US
United States v Moore	923 F .2d 910 (1st Cir. 1991)	US
US v Cestnik	36 F .3d 904 (10th Cir. 1994)	US
US v DeGeorgia	420 F .2d 889 (9th Cir. 1969)	US
US v Dioguardi	428 F .2d 1033 (2d Cir. 1970)	US
US v Linn	880 F .2d 209 (9th Cir. 1989)	US
US v Orozco	590 F .2d 789 (9th Cir. 1979)	US
US v Safavian	435 F. Supp. 2d (DCC 2006)	US
US v Sanders	749 F .2d 195	US
US v Scholle	553 F .2d 1109 (8th Cir. 1997)	US
US v Thomas	78 AFTR .2d 52 96 (9th Cir.)	US
US v Vela	673 F .2d 86, 90 (5th Cir. 1982)	US
Used Car Importers of Ireland v Minister for Finance	[2006] IEHC 90	Irl
Volkering and Others v District Judge Haughton and Another	[2005] IEHC 240	Irl
Walsh v National Irish Bank Ltd	[2007] IEHC 325	Irl
Waterhouse v Baker	[1924] 2 KB 759	Eng
Waugh v British Railways Board	[1980] AC 521	Eng
White v Taylor	[1969] 1 Ch 150	Eng
Williams v Summerfield	(1972) 2 QB 512	Eng
XAG v A Bank	[1983] 2 All ER 464	Eng

INTRODUCTION

Background to the Consultation Paper

1. This Consultation Paper forms part of the Commission's *Third Programme of Law Reform 2008-2014*[1] and is one of three projects concerning aspects of the law of evidence. In 2008, the Commission published a *Consultation Paper on Expert Evidence,*[2] and this Consultation Paper is being followed by a *Consultation Paper on Hearsay in Civil and Criminal Cases.*[3]

2. Documentary evidence is an essential element in nearly all litigation, whether civil or criminal. The traditional law of evidence has tended to treat oral evidence more favourably than documentary evidence especially where adduced without accompanying oral testimony. As documentary evidence has become more common, the traditional exclusionary approach of the law of evidence to documents gradually gave way to a category-by-category inclusionary approach. These categories of documents would then avoid the strict application of the exclusionary rules of evidence. The law as it currently stands has, therefore, developed a number of inclusionary exceptions to accommodate documentary evidence. In recognition of this, the Oireachtas enacted the *Criminal Evidence Act 1992* which provides for an inclusionary approach to documentary evidence in criminal proceedings, thus placing some of these exceptions on a statutory footing. In that respect, therefore, an important aspect of this Consultation Paper is to explore whether a similar approach should be applied in civil proceedings.

3. For the Commission, a second key aspect of the Consultation Paper is to examine to what extent the principles and rules of the law of evidence should apply not only to traditional hard-copy, paper-based documents, but also to electronic and automated documentary evidence. As the Consultation Paper makes clear, the Commission considers that a technology-neutral approach should be adopted to the greatest extent possible, so that the term "documentary evidence" should, in general, apply to traditional paper-based documents and to electronic documents. In this respect, the Commission's proposed "technological-neutrality" would mean that there would be no fundamental differences in the law of evidence between traditional documentary evidence and electronic evidence, and that there would be no evidential

---

1 *Third Programme of Law Reform 2008-2014,* Project 7. Project 7 in the Third Programme commits the Commission to examine Documentary and Electronic Evidence.

2 LRC CP 52-2008. See *Third Programme of Law Reform 2008-2014*, Project 11.

3 See *Third Programme of Law Reform 2008-2014,* Project 8.

preference applied to any particular technology or mechanical device in adducing documentary evidence.

4. This is not to imply that technology can be applied without regard to form. It means, rather, that the way the law would apply to technological choices should be as certain as possible and those choices are made for clearly articulated reasons.

5. In particular, the Commission examines to what extent specific concerns as to proof of execution, authentication and verification may involve different considerations where electronic evidence, as opposed to traditional forms of documentary evidence, is being considered.

Outline of the Consultation Paper

6. In Chapter 1 the Commission examines the scope of the basic unit of documentary evidence; "the document". The Commission examines the evolution of "the document" from a "thing" by which to convey information to an all-embracing concept incorporating the output of mechanical processes and digital devices as well as traditionally understood paper based records. The Commission proceeds to construct a new working definition of a "public document" taking into account the modern meaning and extension of such documents. Chapter 1 also includes a short glossary of electronic terms which are used throughout the Consultation Paper and which play a part in the discussions on electronic and automated documentary evidence.

7. Chapter 2 examines the key principles of the law of evidence which have a bearing on documentary evidence, in particular the overarching consideration of relevance and the factors involved in determining the evidential weight to be attached to a document once it has been admitted in evidence. The Chapter also outlines the traditional preference in the law of evidence for oral testimony. This is done in the context of the emerging document-driven (both paper and electronically derived) and information-driven society and the introduction of the paperless office and how this has affected the collation, generation and maintenance of information. The chapter addresses how the traditional exclusionary approach of the law of evidence to documentary and electronic evidence continues to affect how evidence is currently introduced in courts. The Commission discusses the exclusionary rules of evidence, with particular emphasis on the Best Evidence Rule which is the primary evidential rule that serves to exclude otherwise relevant documentary evidence based on the premise that it is not an original document. This operates to exclude secondary evidence introduced in its place where no original source material is available or discernable unless this evidence can be drawn within one of the (quite numerous) exceptions to the Rule. The Commission has provisionally concluded that the Best Evidence Rule no longer serves a clear purpose in the

law of evidence and ought to be abolished. The Commission also briefly discusses the application of the hearsay rule to written statements (documentary hearsay), which is explored in more detail in the forthcoming *Consultation Paper on Hearsay in Civil and Criminal Cases.*[4]

8. Chapter 3 discusses public documents as one of the main exceptions to the exclusionary rules of evidence. Public documents are deemed to be prima facie admissible in evidence and do not, therefore, involve a breach of the Rule Against Hearsay. The Chapter examines the various forms of public documents which are currently admissible on this basis, notably legislation, records of vital statistics (such as births, marriages and deaths) and documentary evidence of certain professional qualifications. The Chapter examines the characteristics which determine whether a record is a public document so as to avoid the strict application of the exclusionary rules of evidence. The Commission concludes the chapter by contrasting the approach taken to public documents with that taken to private documents. The Commission provisionally recommends that the distinction drawn between public and private documents for the purposes of admissibility as evidence should be retained.

9. In Chapter 4 the Commission examines business documents and records as another of the main exceptions to the exclusionary rules of evidence. The Chapter proposes a new definition of "business record", which would build on existing arrangements, notably those involving the records of financial institutions, based on the *Bankers Books Evidence Acts.* The Chapter places emphasis on how such documents are held or "kept" electronically, including in the context of the detection of fraud and in anti-money laundering legislation.

10. Chapter 5 considers the approach of the law to the authentication of documentary evidence. Assuming, as the Commission has provisionally recommended, that the Best Evidence Rule is to be abolished, the regulation of evidence shifts to a more inclusionary approach, and the next step is to establish the authenticity of the documents. Chapter 5 examines the cornerstone of authenticity for the purposes of admissibility, which is the laying of a suitable foundation upon which to ground evidence. The Commission examines whether its proposed legislative framework would include a higher foundation requirement for electronic and automated documentary evidence. The Commission discusses the factors for adjudicating on the authenticity of secondary evidence of the contents of documents. In this respect, the Commission concludes different standards should not apply as between traditional documentary evidence and electronic and mechanically derived evidence.

---

[4] See *Third Programme of Law Reform 2008-2014,* Project 8.

11. Chapter 5 also addresses the difficulty of categorising electronic and automated documentary evidence, which can be regarded as real evidence or documentary hearsay depending on the level of manual input and human agency involved. Where the evidence has been inputted into an electronic database and the device has essentially been used as an electronic filing cabinet with the aid of manual human intervention, the admissibility of the evidence can be determined in accordance with the rules governing hearsay and its exceptions. Difficulties arise where the electronic evidence is automatically generated within the computer matrix of the mechanical device. This is one example where the Commission has needed to consider electronic and automated documentary evidence separately from traditional documentary evidence.

12. In Chapter 6, the Commission analyses how to authenticate specific pieces of electronic documentary evidence. Electronic records are seen as being more susceptible than their paper counterparts to undetectable modification, whether consciously or as a result of an unintended oversight. The Chapter discusses different types of electronic documents which may emerge from a single initial device. This includes video and audio recordings, and the subtle but distinct differences between analogue and digital photographs and how these are to be authenticated. The Chapter also discusses telephone records as admissible evidence, and whether they constitute real evidence or documentary hearsay. It discusses the admissibility of secondary documentary evidence such as transcripts of recordings and translations, and the purpose for which they are received (for example to support oral expert testimony or as a procedural tool against witness intimidation). The Commission also examines questions surrounding automated documentary evidence and the authentication of computer evidence that can be altered (mutable evidence).

13. This Chapter also examines the procedural aspects of the discovery process with particular reference to electronic documents, in particular how to approach discovery where a document has been erased and where it may be necessary to re-generate or create new documents if needed. The Commission examines briefly the costs and burdens involved in blanket disclosure of voluminous electronic documents and how to streamline the process, which permits the presentation of electronic evidence electronically.

14. Chapter 7 focuses on certification for the purposes of verification of electronic documents and explores whether the law should adopt a uniform means of achieving this. The Commission discusses what constitutes a traditional signature and also an electronic signature. The Commission notes that existing legislation, notably the *Electronic Commerce Act 2000*, differentiates between an electronic signature simpliciter and an advanced electronic signature. The Commission explores the suitability of electronic

signing as a means by which to verify and authenticate electronic documents to achieve legal certainty.

15. Chapter 8 comprises a summary of the provisional recommendations made in the Consultation Paper.

16. This Consultation Paper is intended to form a basis for discussion and therefore all the recommendations made are provisional in nature. The Commission will make its final recommendations on the subject of documentary and electronic evidence following further consideration of the issues and consultation with interested parties. Submissions on the provisional recommendations included in this Consultation Paper are welcome. To enable the Commission to proceed with the preparation of its final Report, those who wish to do so are requested to make their submissions in writing by post to the Commission or by email to info@lawreform.ie by **31 March 2010**.

CHAPTER 1 DEFINING "DOCUMENT" AND "PUBLIC DOCUMENT"

1.01 In Part A of this Chapter, the Commission examines the scope of the basic unit of documentary evidence - "the document" and the associated concept of "records." The Commission examines the evolution of "the document" from a "thing" by which to convey information to an elastic concept incorporating the output of mechanical processes and digital devices as well as traditionally understood paper based records. The Commission also explores the definition of the concept of a "record" for evidentiary purposes. This encompasses not just records kept by private entities but also the increasingly important "public records" that arise in an increasingly complex and regulated society such as Ireland. Thus in Part B the Commission proceeds to construct a new working definition of a "public document" taking into account the modern meaning and extension of the documents in question. In Part C the Commission introduces electronic terms which are used throughout the Consultation Paper. These act as a point of reference for the e-documentary concepts discussed and upon which the later discussions on electronic and automated documentary evidence are premised.

A Defining a Document and a Record in the Law of Evidence

1.02 With the ever-increasing amount of documentary material coming before the courts it is of great importance to provide a clear definition of a "document" for the purposes of admitting these as documentary evidence. The relative position of a given piece of evidence will be greatly affected should it not fall within the definition of a "document." The basic unit of documentary evidence, the "document" itself, therefore requires detailed investigation. With the growth and expansion of what has now come to be accepted as a "document", it is important to examine how it has evolved beyond the traditional paper product to incorporate different media.

(1) The "Document" at Common Law

1.03 The concept of a document for the purposes of English common law was described in 1908 by Darling J in *R v Daye*[1] as comprising "any written

[1] [1908] 2 KB 333.

thing capable of being evidence". This embodied the long established 18th century view of a documentary record as an instrument; a thing, capable of conveying evidence. This also attempted to instil the definition with a certain degree of longevity by not assigning an unduly prescriptive definition to the term "document".

(2) The wide scope of electronic evidence

1.04 At common law, therefore, a document was described as anything upon which information could be visibly inscribed with recognisable and legible characters. The object or medium upon which these characters were inscribed was itself unimportant so long as it was intelligible and information could be gleaned from it by the human eye. This did not anticipate the advent of computer disks or other modern information storage devices, and so the ongoing development of technological innovation therefore required significant adjustment to the common law definition of a "document."

1.05 In general terms, electronic evidence can include any data generated or stored in digital form whenever a computer is used. It includes information manually entered into an electronic device by an individual, information generated in a computational transaction or a response to a request by an individual, where an electronic device generates information acting as an automaton, or information produced and stored where a device processes information within its matrix. Electronic documentary evidence is, therefore, any information captured, generated or maintained in databases, operational systems, applications programmes, computer-generated models which extrapolate outcomes, electronic and voice mail messages and even instructions held inertly within a computer memory bank.[2]

1.06 The law of evidence must, of course, continue to accommodate the traditional notion of a document as any written thing capable of being evidence, since such documents will continue to be relevant to court proceedings for the foreseeable future. The Commission also recognises, however, that this concept of document must also be updated in a unified legislative framework to accommodate electronically generated information capable of presentation in a permanent legible form. This would serve to bridge the definitional gap between manually executed and electronically produced documentary records capable of being admitted as evidence in legal proceedings.

(3) Statutory definitions of "document" in Irish law

1.07 The discrete circumstances of specific cases meant that the common law (judge made law) was not always capable of extending itself to take adequate account of electronic innovation. This led to the enactment of

---

2 US Manual for Complex Litigation, § 21.446 (3rd ed, 1995).

legislation which adapted the view of a document to one which was recognised as essentially anything with distinguishable characters on it. This extended the traditionally held view of a document set out by Darling J in *R v Daye*[3] of a "document" as any written thing capable of being evidence which was broadened by analogy beyond the traditionally held notion of a paper-based record to include different media. Darling J acknowledged that "it is immaterial on what the writing may be inscribed" suggesting, even in 1908, allowances for future progressions in the field of information retention.

1.08 The definition was indeed overtaken by advances in the of data collation and retention and courts will now accept as valid any item which gives information as opposed to an item on which writing can be inscribed. This view was judicially endorsed in Ireland by the Supreme Court in 1979 in *McCarthy v O'Flynn*[4], to the effect that "a document is something which teaches or gives information or a lesson or an example of construction". The Supreme Court held that an X-ray sufficiently constituted a document for the purposes of discovery of documents in civil proceedings.

1.09 Statutory definitions are broader than the common law definition, even as expanded to include X-rays (as in the *McCarthy* case), but as discussed below they do not attempt to be exhaustive.

1.10 The term "document" and other associated terms have been defined for specific purposes in recent Irish legislation. These definitions often accommodate the traditional document and modern electronic forms of evidence. Thus, section 2 of the *Criminal Evidence Act 1992* defines a document as "including" (indicating clearly this is not an exhaustive list):

> "(i) a map, plan, graph, drawing or photograph, or
>
> (ii) a reproduction in permanent legible form, by a computer or other means (including enlarging), of information in non-legible form."

1.11 Section 2 of the 1992 Act also defines "information" as including "any representation of fact, whether in words or otherwise".

1.12 It is also notable that other legislation operating in the criminal law setting has been updated to take account of technological developments. Thus, the definition of a document in section 2 of the *Offences Against the State Act 1939* had originally envisaged a document as an exclusively paper based means of communicating information. This was updated by the *Offences Against the State (Amendment) Act 1972* to take account of technological

---

3 [1908] 2 KB 333 at 340.

4 [1979] IR 127.

developments at that time, including tape recordings.[5] While the updated definition in the 1972 Act may have been sufficient for its time, such a technologically prescriptive form runs the risk of becoming quickly outmoded and overtaken by innovation. In that respect, the Commission emphasises the need for a definition that is future proofed.

1.13 The most recent legislative definition of a document is contained in the *Criminal Justice (Surveillance) Act 2009* which defines a document as "including":

> "(a) any book, record or other written or printed material in any form, and
>
> (b) any recording, including any data or information stored, maintained or preserved electronically or otherwise than in legible form."

1.14 The Commission notes that the overwhelming majority of legislative definitions of documents in Irish law have been confined to the criminal law sphere. It may well be that, in the context of civil law proceedings, the decision of the Supreme Court in *McCarthy v Flynn* indicates that the courts would not have great difficulty in expanding the traditional concept of "document" to take account of technological developments. Nonetheless, it remains the case that, at least in legislative terms, the law of evidence has expressly been advanced as regards criminal law to a greater extent than the civil law.

1.15 Acts such as the *Criminal Evidence Act 1992* and the *Criminal Justice (Surveillance) Act 2009* have clearly developed the definition of "document" to take account of technological innovations. The Commission's purpose in preparing this Consultation Paper is to recommend a uniform, technologically neutral, definition which would encompass both manual and electronic and automated documentary evidence. From this perspective it is perhaps arguable that the use of the term "document" could itself prove a limitation to the recognition of digital evidence and could conceivably cause difficulties when attempting to include electronic and automated instruments.

---

[5] Section 5 of the *Offences Against the State (Amendment) Act 1972* included in its definition "(c) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom, and (d) any film, microfilm, negative, tape or ether device in which one or more visual images are embodied (whether with or without sounds or other data) so as to be capable (as aforesaid) of being reproduced therefrom and a reproduction or still reproduction of the image or images embodied therein whether enlarged or not and whether with or without sounds or other data."

1.16 In considering the language to use in any proposed legislative framework, it is useful to examine the legislative provisions which define the concept of a "record". For example, section 2 of the *Freedom of Information Act 1997* defines a "record" in great detail as "including":

> "any memorandum, book, plan, map, drawing, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (within the meaning of the Data Protection Act, 1988) are held, any other form (including machine-readable form) or thing in which information is held or stored manually, mechanically or electronically and anything that is a part or a copy, in any form, of any of the foregoing or is a combination of two or more of the foregoing."

1.17 In 2001 in *Minister for Justice, Equality and Law Reform and the Courts Service v Information Commissioner*[6] the High Court examined derivatives and photocopies in the context of the relevant provisions of the *Freedom of Information Act 1997*. The Court adopted an inclusionary stance and noted that "taking a simple example from that definition of a record (under section 2 of the 1997 Act) a copy of a document is a record: clearly originality is not a necessary ingredient in a record. It cannot be said that the person who creates the copy of the document which is by the statutory definition a record is not the creator of that record." Finnegan J was of the opinion that as regards the compilation of documents under section 6 of the *Criminal Procedure Act 1967* [7] even where these documents were presented as consisting solely of photocopies of documents prepared elsewhere and furnished for the book of evidence, these photocopies would suffice as records. So long as the Director of Public Prosecutions who had created the documents retained control of the original statements and other source documents, photocopies or derivatives would be acceptable.

1.18 As already noted, while criminal proceedings are well accommodated by specific pieces of legislation, there is no general definition of what comprises a document for the purposes of civil proceedings (or, indeed, for the purposes of all criminal proceedings). At this stage of the Consultation Paper, the Commission notes that a number of choices or options are possible. Thus, the term "document" could be interpreted broadly to link it more precisely with new technological concepts. It could also incorporate a more abstract term such as the concept of "records." The concept might also be extended into an umbrella term encompassing all structured units of recorded information. Even

---

6 High Court 14 May 2001.

7 As amended by section 12 of the *Criminal Evidence Act 1992*.

at this stage, the Commission is conscious in this respect that great care must be taken in order that any definition does not become unwieldy.

(4) Statutory definitions of documents and records in the English Criminal Justice Act 2003

1.19 The English *Criminal Justice Act 2003* is the most recent legislative approach to address the admissibility of documentary evidence in England and Wales. Previous legislative attempts to address this area have included the *Criminal Evidence Act 1965*, followed by the *Police and Criminal Evidence Act 1984* (PACE) and the *Criminal Justice Act 1988*. Indeed, it should be noted that these previous Acts have influenced the content of Irish legislation, such as the *Criminal Evidence Act 1992*, discussed above.

1.20 The English 2003 Act also reflected the outcome of case law in the English courts. For example, in *R v Ewing*[8] the question was whether the printout of a computer displaying the transaction history of a bank account was admissible as documentary evidence under the English *Criminal Evidence Act 1965*. The English Court of Appeal described the computer printout as an element of "a device by means of which information is recorded or stored" and which therefore fell within the *Criminal Evidence Act 1965* because without this document "there was no other means of discovering the information" recorded in it.[9]

1.21 In *Darby v DPP*[10] a question arose as to whether the data recorded by a speed gun, the "GR Speedman," were capable of being documentary evidence for the purposes of section 69 of the *Police and Criminal Evidence Act 1984*. The appellant submitted that the data were inadmissible if they were held to constitute a document. It was held that the speed gun was a computer for the purposes of the English legislation and that the visual image of the information recorded was a document produced by a computer.

1.22 The English *Criminal Justice Act 2003* conforms to current non-prescriptive forms of definition and describes a document very succinctly as "anything in which information of any description is recorded."[11]

---

8 [1983] QB 1039.

9 O'Connor LJ at 1050-1051.

10 Queen's Bench Division, 4 November 1994, QBD.

11 *Criminal Justice Act 2003,* section 134 (1) and *Civil Procedure Rules* Part 31.4.

(5) The Definition of a document in the Australian Uniform Evidence Act 1995

1.23 The definition in Ireland's *Criminal Evidence Act 1992* is extensive, although as noted, because it uses the word "includes" it clearly is not prescriptive. The 1992 Act cannot, however, be said to be future proofed so as to extend beyond the common law barriers of anything tangible with visibly inscribed characters. In this respect, legislative developments in Australia in 1995 provide a useful model. The Australian Uniform Law Commissioners, who represent the federal (Commonwealth) and State governments, developed a *Uniform Evidence Act* which was implemented in the federal and (some of the) state legislatures in 1995. Each of these *Uniform Evidence Acts* enacted in 1995 defines "document"' as any "record of information," including:

> (a) anything on which there is writing; or
> (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or
> (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or
> (d) a map, plan, drawing or photograph.

1.24 This wider definition of the term "document" has been said to "greatly increase the flexibility of the law to admit the contents of documents into evidence".[12]

1.25 The *Uniform Evidence Acts* have also gone further and reformed and updated the law on documentary evidence in relation to cross-examination on documents,[13] refreshing memory from documents[14] and the means of proving attested documents.[15]

---

12 J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002), 105.

13 *Uniform Evidence Act 1995* sections 40-42.

14 *Uniform Evidence Act 1995* section 27. See also V Bell, '*Documentary Evidence under the Evidence Act 1995 (NSW)*' (2001) 5 The Judicial Review 1.

15 Where the validity of a document depends on it having been properly attested, at common law it was necessary to prove this fact by calling one of the attesting witnesses to testify, unless the witnesses were unavailable or a presumption of validity applied. Section 149 of the 1995 Act removed this requirement.

(6) An Expanded Notion of an Electronic Document in New Zealand

1.26 The New Zealand *Evidence Act 2006* introduced an expanded definition of a document. It operates on the understanding that there is a single, unified concept of a document which incorporates both hard copy and electronic documents. The traditional concept of a document is incorporated as including any material bearing interpretable signs or symbols, sounds or images or writing that identifies or describes a thing.[16] In this sense there has been an attempt at future proofing the definition particularly with the inclusion in the definition of:

> "information electronically recorded or stored, and information derived from the information".[17]

(7) The definition of documentary evidence in the 1996 UNCITRAL Model Law on Electronic Commerce

1.27 Another useful definition is that developed by the United Nations Commission on International Trade Law (UNCITRAL). The UNCITRAL 1996 Model Law on Electronic Commerce refers to electronic materials producing electronic and automated documentary evidence in the form of "data messages". The1996 Model Law defines electronic or computer information and includes information:

> "generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy."[18]

---

16 Under Part 1 section 4 of the *Evidence Act 2006* a "document" means—

(a) any material, whether or not it is signed or otherwise authenticated, that bears symbols (including words and figures), images, or sounds or from which symbols, images, or sounds can be derived, and includes—

(i) a label, marking, or other writing which identifies or describes a thing of which it forms part, or to which it is attached:

(ii) a book, map, plan, graph, or drawing:

(iii) a photograph, film, or negative; and

(b) information electronically recorded or stored, and information derived from that information.

17 *Evidence Act 2006*, Part 1 (4).

18 UNCITRAL Model Law on Electronic Commerce (1996), article 2 (a).

(8) Reforming the Definition of a "Document"

1.28 As already discussed, it is clear to the Commission that a revision of the definition of "document" for the purposes of the general law of evidence as it operates in both civil and criminal proceedings is necessary, in particular to take account of changing technology. The definition should embrace the concepts of "writing" and a "record," which existing Irish legislation has sometimes defined in extremely prescriptive terms, but which does not even purport to be exhaustive. The concepts of "writing" and "record" are also, at least superficially, narrower than the concept of "document", which linguistically incorporates a wider array of written material.

1.29 Bearing in mind the apparent success of the examples of definitions of "document" from other States, such as Australia and New Zealand, the Commission does not consider that electronic and automated documents require a separate definition. In Chapter 5, the Commission addresses a related, but separate matter: whether electronic and automated documentary evidence may require a different, more nuanced, test to assess their reliability for admissibility purposes.

1.30 The Commission considers that it is essential to adopt a definition which is not so time-specific and medium-specific that it would not be able to embrace new technologies as they emerge, as was the case with the 1970s-specific update in the *Offences Against the State (Amendment) Act 1972* discussed above. This would avoid the risk that the definition would become obsolete, and thus also avoid, as far as possible, unnecessary future piecemeal statutory amendments.

1.31 The Commission is of the view that "document" defined along these lines would be capable of evolving to take account of future electronic devices producing anything in legible form which can be adduced as evidence. The Commission is therefore of the opinion that the long-established definition in the law of evidence of "documentary evidence" as being a thing in legible form that is capable of being adduced in evidence should be placed within a statutory framework and supplemented by the addition of references to electronic and automated documents and records. In light of this the Commission favours a redefining of the concept of a "document" as "anything in which information of any description is recorded". The Commission also recommends that this definition of "document" is to be understood as combining electronic, automated as well as hard copy traditional documents and that this definition would apply to both civil and criminal proceedings.

1.32 The Commission provisionally recommends that the long-established definition in the law of evidence of "documentary evidence" as being a thing in legible form that is capable of being adduced in evidence should be placed

within a statutory framework and supplemented by the addition of references to electronic and automated documents and records.

1.33 The Commission provisionally recommends that "document" should be defined for the purposes of the law of evidence as "anything in which information of any description is recorded". The Commission also provisionally recommends that this definition of "document" is to be understood as combining electronic, automated as well as hard copy traditional documents and that this definition would apply to both civil and criminal proceedings.

1.34 This approach suggests, in the Commission's view, that all the elements incorporated into, for example, the Australian *Uniform Evidence Acts* enacted in 1995 and those already present in the Irish *Criminal Evidence Act 1992* should be present in any general legislative framework. It should also incorporate the approach taken in the 1996 UNCITRAL Model Law on Electronic Commerce.

1.35 This definition would involve a move towards a non-prescriptive and technologically neutral definition, which would be capable of adapting to new technologies as they emerge. The Commission is thus of the opinion that the law of evidence in its application to documentary evidence should, in general, adopt a general technologically-neutral approach, in which the essential rules of admissibility should apply equally to traditional forms of manually created documents and to electronic and automated documents and records.

1.36 The Commission provisionally recommends that the law of evidence as it applies to documentary evidence should adopt a technologically-neutral approach, in which the essential rules of admissibility should apply equally to traditional forms of manually created documents and to electronic and automated documents and records.

B Defining a "Public Document"

1.37 In addition to the type of documents already discussed, such as contracts and X-rays, civil and criminal cases often involve reference to public documents, such as birth and marriage certificates or other extracts from public registers. The details of the method by which public documents are proved in the law of evidence are addressed by the Commission in Chapter 3. For present purposes, the Commission outlines a proposed definition of "public document" for incorporation into the Commission's proposed statutory framework.

1.38 A well-established general definition of "public document" is that it is a record issued for public knowledge. Public documents are, in accordance with the common law and relevant statutory provisions (such as the *Documentary Evidence Act 1925*, which is discussed in detail in Chapter 3), generally admissible as evidence and as proof of their contents, subject to rebutting

evidence. Certain public documents may also be admitted in evidence on the basis that they are judicially noticed, that is, that because their contents are so widely known that they are incapable of successful challenge by any litigating party.

1.39 As with "document", in the Commission's view there is a need for a clear definition of "public record". Case law has, over the years, established certain characteristics, the presence of which would identify a documentary instrument as a public record. These are considered in greater detail in Chapter 3[19] but it is sufficient for present purposes to say that the relevant criteria are well-established.[20] They provide that in order for a record to be classed as a public record for the purposes of the law of evidence there must be an initial public duty to record the information and to do so in an unbiased and honest manner.[21] The information recorded must be of concern to the public and also be public in nature.[22] The data recorded must be retained[23] and further to this it must be properly maintained and held so as to be available to public inspection.[24] The Commission considers that these criteria are sufficiently well-established and wide-ranging in scope that they are suitable for inclusion in the proposed statutory framework.

1.40 The Commission, accordingly, provisionally recommends that a "public document" should be defined as "a document retained in a depository or register relating to a matter of public interest whether of concern to sectional interests or to the community as a whole, compiled under a public duty and which is amenable to public inspection."

1.41 The Commission provisionally recommends that a "public document" should be defined as "a document retained in a depository or register relating to a matter of public interest whether of concern to sectional interests or to the community as a whole, compiled under a public duty and which is amenable to public inspection."

---

19 See below paragraph 3.11.

20 See further Tapper, *Cross and Tapper on Evidence*, 11th Ed, Oxford University Press, 2007, p 633.

21 *Doe d France v Andrews* (1850) 15 QB 756.

22 *R v Halpin* [1975] QB 907.

23 *Heyne v Fischel & Co* (1913) 30 TLR 190, *Mercer v Dunne* [1905] 2 Ch 538, *White v Taylor* [1969] 1 Ch 150.

24 *Lilley v Pettit* [1946] KB 401.

C Electronic Terms and E-Document Characteristics Discussed in the Consultation Paper

1.42 In the course of this Consultation Paper, the Commission uses the broad term "electronic and automated documents" to indicate all means of electronic capture and transfer of information. This includes information transferred or held or generated using electronic technology (for example, email) or information held or generated using magnetic technologies (for example, magnetic disks including first generation phone cards) or optical disk technologies (for example, CD-ROMs). While these are often used together by the Commission to indicate a generic e-document, there are times when the term is broken into its component parts where, for example, the law is being investigated from different perspectives in the law of evidence. Because some of these terms are relatively new, the Commission considered it might be useful to provide a glossary of terms used in the Consultation Paper. It should be noted that these terms are discussed here for informational purposes only.

(i) Asymmetric Cryptosystem

1.43 An asymmetric cryptosystem is an electronic system which can be used to generate a secure key pair for electronic communications and transacting and which consists of a private key for creating an electronic signature and a corresponding public key for verifying the electronic signature.

(ii) Certification Authority

1.44 A certification authority is a trusted third party that vouches for the identity of an individual or business enterprise or server and signs a certificate.

(iii) Certificate

1.45 A certificate is a specially formatted electronic document signed by a trusted third party and its function is to attest to the validity of the contents of the document in question.

(iv) Electronic Signing.

1.46 An electronic signature is, at its most basic level, a code attached to an electronic document that reliably identifies the author or sender, and verifies that the document has not been tampered with. Specific types of electronic signatures are statutorily defined, and these are discussed in the Consultation Paper.

(v) Hash Digest Function.

1.47 Hash digest function means an algorithm mapping or translating one sequence of bits into smaller set for the purposes of rendering it computationally impossible that a record can be reproduced from the hash result produced by the algorithm.

(vi) Meta-data

1.48 Meta-data is the data about data and involves examining the electronic trail documenting the provenance and chain of custody from inception to end-document. Meta-data is visible throughout the electronic document and provides a wealth of knowledge. It may include the user's name or initials or the name of a company, the name or assignation of the computer on which the file was created, the network server or hard disk where the file has been recorded or saved as well as other file properties. It may also contain summary information about the provenance of the electronic document including the time of creation or transmission of the document or equally the time and date of any modifications made. It is an amalgam of information buried within the electronic record of the document and can track the development of a document from inception to transmission far more rigorously than the trail of a paper document may be identified.

(vii) Private Key.

1.49 A private key is an encryption device used by a limited number of communicating parties to decrypt data encrypted with a public key.

(viii) Public Key.

1.50 A public key is an encryption device known to all users, used to encrypt data in such a way that only a specific user can decrypt it.

(ix) Spoliation

1.51 Spoliation refers to the withholding, hiding or destruction of evidence relevant to legal proceedings.

CHAPTER 2 THE EXCLUSIONARY RULES OF EVIDENCE RELEVANT TO DOCUMENTARY EVIDENCE

2.01 In this Chapter, the Commission discusses the general rules of the law of evidence and the exclusionary rules of evidence as they apply to documentary evidence and which operate to exclude secondary evidence from being admitted. This includes the relevant exclusionary rules of evidence, the best evidence rule and the rule against hearsay as they apply to documentary evidence. The Commission examines this both from a traditional paper-based view as well as the application of the rules to the newly emerging body of electronically-generated documentary instruments.

2.02 In Part A, the Commission discusses the law of evidence as it applies to documentary and electronic and automated documentary evidence. It looks at the nature of documentary evidence as evidence, as opposed to oral evidence. Part A then discusses the rules of evidence and the concept of relevance as the basis on which the admissibility of a piece of documentary evidence depends. This is the primary focus of admitting documentary evidence as admissibility is purely a function of relevance. Apportioning the weight of a given piece of evidence is also considered and the Commission notes that, where other exclusionary factors are not in issue, the process of admitting documentary evidence is far more simplified. It is admitted where relevant, with all other considerations going toward establishing the weight to be attached to it.

2.03 In Part B the Commission discusses the exclusionary rules of evidence, with particular emphasis on the Best Evidence Rule as the primary rule which serves to exclude otherwise relevant documentary evidence based on the premise that it is not an original document, and which operates to exclude secondary evidence in its place unless this evidence can be drawn within one of the exceptions to the Rule. The Commission discusses the origin and evolution of the Best Evidence Rule, the waning of judicial support for it, and its ultimate decline in the regulation of electronic evidence and how it operates to exclude copies of documents in proceedings. The Commission examines the arguments for and against the retention or abolition of the rule. This Part also explains the nature of electronic and automated documentary

evidence as documentary evidence, the status of copies and technological devices as "documents".

2.04 Part C examines the various exceptions to the exclusionary rules in Ireland. These include: loss, destruction, impossibility of physical production, the public documents exception and the business records exemption. The Commission examines the basis for these inclusionary exceptions against the background of the exclusionary Best Evidence Rule.

2.05 In Part D, the Commission examines the abolition of the Best Evidence Rule in other jurisdictions and the status of electronic documents there. The Commission ends this Part by concluding that the Best Evidence Rule no longer serves a clear purpose in the law of evidence and ought to be abolished.

2.06 In Part E, the Commission turns briefly to examine the Rule Against Hearsay both generally and in its interaction with the Best Evidence Rule in the context of both traditional and electronic and automated documentary evidence This will be discussed in more detail in the Commission's forthcoming *Consultation Paper on Hearsay in Civil and Criminal Cases.*[1]

2.07 Part F discusses the shifting focus of the law of evidence to accommodate both traditional and electronic and automated documentary evidence. The Commission concludes that the Best Evidence Rule in its application to both electronic and traditional evidence in both civil and criminal proceedings should no longer apply as a determinant of admissibility when adducing documentary evidence.

A The Law of Evidence and Documentary Evidence

(1) How Oral and Documentary Evidence is Given in Court

2.08 A large amount of civil and criminal litigation in Ireland is conducted using oral evidence, with witnesses offering testimony, being examined by their representatives and in turn cross-examined by opposing counsel. Oral testimony is, therefore, presumptively admissible and the techniques of examination and cross-examination are primarily aimed at determining the weight, or reliability to be attached to the person's evidence. By contrast, documents are subject to a higher level of initial threshold scrutiny as to admissibility. They must, in general, be proven by witnesses in order to be deemed admissible as evidence of their contents, unless otherwise agreed to by the parties.

---

1 *Third Programme of Law Reform 2008-2014,* Project 8.

2.09 In the vast majority of cases, of course, there will be no serious objection to the documentary evidence and where questions of admissibility do arise these are often on the grounds of relevance. It is important to note that documentary evidence may be offered in an effort to have that document admitted for the limited purpose of proving merely that it was written, sent and received, not for the wider purpose of evidence of the truth of its contents. It must be remembered that if a document is introduced to prove the truth of its contents, it is classified as documentary hearsay and is, generally, inadmissible unless it falls within one of the inclusionary exceptions such as "public documents."

2.10 Another important matter which the Commission discusses below is how the law of evidence approaches original documents and copies of documents. In this respect, the law of evidence takes a common sense approach. If the original document, such as a written contract, is available, it should be produced: this is called the Best Evidence Rule. If, however, the original is unavoidably unavailable, a court will often accept alternative evidence, such as a certified copy or direct oral testimony by a witness who was present when the document was made: this is called Secondary Evidence. In practice, it is relatively rare for an objection to be taken to the introduction of a copy (in the context of electronic documents, often called a derivative) in place of an original document, in strict reliance on the secondary evidence rule. Where such an objection does arise it is usually an attempt to gain a tactical forensic advantage by, for example, causing the person who wishes to introduce the copy of the document to call a witness to explain the absence of the original, a person who will then be liable to cross-examination.

2.11 In general, the rules of evidence concerning documentary evidence, whether traditionally executed paper documents or electronic documents, apply to both civil and criminal proceedings. Indeed, this is true of virtually all rules of evidence. It is notable however, that statutory intervention to date in Ireland to alter the rules of evidence has tended to apply to criminal proceedings only, where the rules governing evidence appear to be more strictly observed.

(2) The Rules of Evidence

2.12 The rules of evidence govern how a litigant will go about proving his case. The rules of evidence are in place to assist the court in its role. The litigant will place evidence before the court which is subject to differing evidential rules and threshold over which it must pass. A litigant must determine how to adduce his evidence. Whether this evidence is in documentary form or otherwise the court will assess the evidence as to whether it is admissible and

then seek to weight to the evidence based on its integrity, reliability or the "circumstantial guarantee of trustworthiness"[2] and probative value.

2.13 It should be noted here that the meaning of the term "reliability" shifts with its context and the rule under consideration. For authentication, reliability means that the record is what it purports to be. For the Best Evidence Rule, reliability means that the record is accurate or has integrity. For hearsay, reliability relates to the truth of the contents of the record.

(3) Relevance

(a) Admissibility as a function of relevance

2.14 There are a very few basic rules of evidence which underscore all subsequent rules of evidence and the exceptions applying to them. A key rule is that all relevant evidence is admissible. Whether a piece of evidence offered is relevant depends on the purpose for which it is intended. It has been said that all other rules of evidence are an exception to the relevance rule.[3] The primary rule of admissibility of evidence is that the evidence offered must be relevant to the issues in the proceedings and will usually be admitted where its probative value outweighs its prejudicial value and unless there is another rule of evidence to exclude it. Consequently evidence which is not relevant will not be admitted unless there is consent between the parties.

2.15 The primary focus in admitting a document, as with any other evidence, will turn on its relevance to the issues being litigated. A classic definition of relevance was advanced by Stephen and has been approved by contemporary academics[4] as meaning that:

> "any two facts to which it is applied are so related to each other that according to the common course of events one either taken by itself or in connection with other facts proves or renders probable the past, present or future existence or non-existence of the other."[5]

2.16 Admissibility is purely a function of relevance and where relevant a document will be admitted regardless of whether it is in documentary form or

---

2 Wigmore, JH. *A Treatise on the Anglo-American System of Evidence in Trials at Common Law,* vol III, 2nd ed. Boston: Little, Brown & Co., 1923, §§ 1420-22. This interpretation of reliability was approved in *R v Smith* [1992] 2 SCR 915, Lamer J at 270.

3 Chalmers, K. "*Towards a more Principled Approach to the Law of Evidence*", from a Convention Paper given to the American Advocates Society in October 1994.

4 McGrath, *Evidence*, Thomson Round Hall, 2005, p 2.

5 Stephen, *Digest of the Law of Evidence*, 12th Ed, McMillan & Co. Ltd., 1907.

electronically generated. Courts are concerned with the probity of potential documents. Where potential evidence is identified as superfluous or irrelevant it will not be entertained. Thus, Kingsmill Moore J stated in *The People (AG) v O'Brien*[6] that evidence is relevant where "it is logically probative".

(b) Determining the relevance of an electronic document

2.17 In determining the relevance of electronic documentary evidence it may be necessary to show that the document is what it purports to be and represents the information which it is suggested as doing. An example of this was expressed in the context of audiotapes so that the provenance of the tape recording must be satisfactorily established before it is played over to the jury. This provenance the authentication for the purposes of admissibility - can be established with regard to electronic documentation by establishing how the document was generated or otherwise brought into existence, coupled with showing the reliability of the processes and the accuracy of the electronic systems or devices which were used to store, transmit or generate the document. A further factor in establishing the reliability and authenticity of an electronic document is to show that the document and its text has not been altered or been subject to any attempted spoliation over the course of its lifetime.

2.18 This means that the document may need to be authenticated by an extrinsic source before it is admissible. A document cannot usually speak for itself and cannot authenticate itself. Consequently the party seeking to rely on a document must adduce evidence that confirms that the document is what it purports to be. Authenticating a document is an exercise of judgment and one of balancing the risks of acceptance against its benefits.[7] Electronic documents present challenges previously unknown and it is necessary to investigate the legal climate in which they operate in order to determine whether the current rules are sufficiently strong to regulate them. This will also reveal whether the current rules can be made flexible enough to accommodate them or whether they require a separate discrete area of the law of evidence to regulate them.

2.19 The evidence required to authenticate a document will be determined in part by the nature of the document in issue. While traditional paper documents may be authenticated by the testimony of the author or by the testimony of a person who witnessed the author sign the document, this may not be suitable for electronic evidence.

---

6 [1965] IR 142 at 151.

7 Gregory, JD, "*Authentication Rules and Electronic Records*" Ontario, Canada Canadian Bar Review, November 2001. Available at www.cba.org.

2.20 In considering the standard of proof required for authenticating digital evidence, the Queensland Law Reform Commission noted some obscurity in the common law:

> "With evidence produced by devices or systems, however, the courts appear to have required that the trial judge be satisfied—presumably, on the balance of probabilities—as to the accuracy of the technique and of the particular application of it."[8]

2.21 Electronic and automated documentary evidence may in turn be authenticated by evidence which confirms that, where a device has been used to produce the evidence, the device used was reliable and accurate.

2.22 While relevant evidence is admissible, the court retains its discretion to exclude otherwise admissible evidence under certain circumstances. What would otherwise qualify as admissible evidence would be excluded where the probative value would not outweigh the prejudicial effect of the document adduced or where the documents run aground on the exclusionary rules of evidence.

(4) Factors Affecting the Weight of the Documentary Evidence (Other than Real Evidence)

2.23 The following are considerations which the court will take into account when estimating the weight to attach to relevant documentary evidence.[9] The court will not only take into account the circumstances

---

[8] *The Receipt of Evidence by Queensland Courts: Electronic Records*, Issues Paper WP No 52 Queensland Law Reform Commission, August 1998.

[9] A coherent legislative framework laying down the matters the court will take cognisance of in considering the weight to be given to hearsay evidence were set out in Section 4 of the English *Civil Evidence Act 1995*;

(1) In estimating the weight (if any) to be given to hearsay evidence in civil proceedings the court shall have regard to any circumstances from which any inference can reasonably be drawn as to the reliability or otherwise of the evidence.

(2) Regard may be had, in particular, to the following:-

(a) whether it would have been reasonable and practicable for the party by whom the evidence was adduced to have produced the maker of the original statement as a witness;

(b) whether the original statement was made contemporaneously with the occurrence or existence of the matters stated;

(c) whether the evidence involves multiple hearsay;

surrounding the creation or transmission of the document and draw any appropriate inferences which would suggest anything about the reliability of this, but will also have regard to whether it would have been reasonable to expect the party adducing the documents to have called upon the maker of the original document to offer oral testimony. The court will have regard to the time lag between the original event which the document records and the correlation between this time and when the original document was in fact produced. The court will further consider whether the document in question involves multiple layers of hearsay or whether indeed the original was a cumulative document which could impact on the reliability of the record. It should be noted that, when approaching the determination of the reliability and weight to be attached to a document, the trier of fact (a judge or jury, as the case may be) will adopt a pragmatic approach to this assessment.

B The Best Evidence Rule; the Rule as to Secondary Evidence of the Contents of a Document

2.24 An exception to the general rule regarding the admissibility of relevant evidence is referred to as the Secondary Evidence Rule. The general effect of this rule is that a party relying on the words used in a document for any purpose other than that of identifying it must adduce primary and original evidence of its contents.

2.25 The rule was developed in relation to documentary evidence and requires that the Best Evidence – the original document - be produced, or that its absence be explained before a copy can be admitted as evidence in its place. This secondary evidence rule was developed before the advent of computer technologies and even before more basic electronics such as photocopiers or even carbon paper became the norm. The rationale for the rule was to protect against the risk of inadvertently receiving errors through the manual copying process, as well as the prevention and detection of fraud.

2.26 There are a number of common law and statutory exceptions to the secondary evidence rule. In these circumstances, the law permits secondary evidence, such as a copy of a document, to be given to prove the contents of a

---

(d) whether any person involved had any motive to conceal or misrepresent matters;

(e) whether the original statement was an edited account, or was made in collaboration with another or for a particular purpose;

(f) whether the circumstances in which the evidence is adduced as hearsay are such as to suggest an attempt to prevent proper evaluation of its weight.

document. These exceptions are not cumulative and it may be that a document will fall within more than one category.

(1) The Best Evidence Rule

(a) Historic Evolution and Consequent Waning of the Best Evidence Rule

2.27 The fundamental principle of the common law is that the best evidence - the original document - must be offered to the court in order to satisfy the requirements of evidential rules. The interaction with the rule against hearsay is therefore clear, because the hearsay rule also prevents a person testifying to the truth of what he has been told by another.[10] This procedural demand for original evidence is undoubtedly one of the more marked attributes of the law of evidence and is essentially related to the means of proving the matters that require proof (originally called the *modus probandi*).

2.28 The Best Evidence Rule can be taken as having for centuries been the prevailing rule regulating the admission of documentary evidence and was a standard feature of the common law mode of proof. The rule can be traced at least to the 18th century with Lord Hardwicke noting in 1745 that the judges "and sages of the law have laid down that there is but one general rule of evidence, the best that the nature of the case will admit."[11]

2.29 The primacy of the Best Evidence Rule can be dated back to Lord Chief Baron Gilbert's late 18th century textbook *Law of Evidence* where he used the rule as part of a unifying theory which placed documentary evidence at the peak of a rigid evidential hierarchy of categories, with public records at the top and which gradually filtered down through other kinds of documentary evidence with oral evidence on the bottom rung. Gilbert was of the opinion that "the first and most signal rule in relation to evidence is this, that a man must have the utmost evidence the nature of the fact is capable of"[12] expanded to mean "the true meaning of the rule of law that requires the greatest evidence that the nature of the thing is this: That no such evidence be brought which *ex natura rei* supposes still a greater evidence behind the power."[13] Bacon's earlier authoritative treatise on English law has it that "it seems in regard to evidence,

---

10 Cross's formulation of hearsay is that: "an assertion other than one made by a person while giving oral evidence in the proceedings is inadmissible as evidence of any fact asserted." *Cross on Evidence* 7th ed 1990, p 42.

11 *Omychund v Barker* (1745) 1 Atk, 21, 49; 26 ER 15, 33.

12 *Gilbert's Law of Evidence* (four volumes), London 1791-6, Dublin 1795-7, at p 4.

13 *Gilbert's Law of Evidence* (four volumes), 16 4th Ed.

to be an incontestable rule, that the party who is to prove any fact must do it by the highest evidence the nature of the thing is capable of."[14]

2.30 Gilbert's approach was heavily criticised in the 19th century by the legal philosopher and political scientist Jeremy Bentham who noted that such an approach effectively consigned all real evidence to a peripheral role and gave insufficient attention to the problems of authentication and reliability routinely associated with documents. Bentham for his part valued oral testimony as the primary evidential force, on the view that "witnesses are the eyes and ears of justice."[15]

2.31 The proposition for the Best Evidence Rule was again expounded by Sir WD Evans in the context of contract law in 1806. He encouraged the development of exceptions to counteract the strictness of the Rule as it otherwise stood. He emphasised a level of flexibility incorporated into the Best Evidence Rule which he thought ought to be relaxed on grounds of either "absolute necessity or as a necessity presumed from the common occurrences… the rule is not so stubborn but that it will bend to the necessities of mankind and to the circumstances not under their control. The rule is adopted only to obviate the fraud of mankind."[16]

2.32 In this chapter the Commission examines the application of this criterion to the proof of documentary instruments identified as sufficiently relevant and proximate to the matters in issue. These are instances of primary evidence and are sufficient as proof of evidence of their own contents. Secondary evidence is a means of proving evidence in a derivative form and it has long been held that through the application of the Best Evidence Rule, no secondary evidence can be admitted until the non-production of the original is explained to the satisfaction of the court.

(b) The Original Document Rule

2.33 It is clear that the admissibility of a 'document' at common law was generally dependent on the production of the unique original of that document, unless one of the exceptions to the secondary evidence rule could be established. At common law the "Best Evidence Rule" was a hurdle placed

---

14 Bacon Abr Evidence 1 Ed 1736.

15 J Bentham, *Introductory View of the Rationale of Judicial Evidence*, (1838-53) cited in J Hunter and K Cronin, *Evidence, Advocacy and Ethical Practice*, Butterworths, 1995.

16 Sir WD Evans in *Pothier on Obligations*, 1806 p148, cited in W Twining, "The Rationalist Tradition of Evidence Scholarship" in *Rethinking Exploratory Essays,* Blackwell (1990), p 35.

before the proponents of a document, the intention of which was to eliminate the possibility of admitting an erroneous fabrication or inaccurate document by requiring a party to introduce the best evidence available which the nature of the case allowed. For this reason the Best Evidence Rule is also commonly referred to as the Original Document Rule. The Best Evidence Rule requires in essence that the content of a documentary tool is only acceptable as evidence when proven by introduction of the original. This rule developed in the 18th century, when pretrial discovery was practically nonexistent and manual copying was the only means of reproducing documents which, owing to human fallibility, resulted inevitably in discrepancies in the replications. The need for the retention of the rule must now therefore be questioned.

(2) The Best Evidence Rule and Electronic Evidence

2.34 In the context of electronic records, the question of what is an original record for the purposes of the Best Evidence Rule is not as clear cut as it is with corresponding paper equivalents. This begs the question of whether the rule as to proof of secondary evidence of the contents of a document should apply at all in relation to electronic records and, if so, whether some clarification is required in that context as to what constitutes an original or a copy of an electronic record.

2.35 One approach would be to reform the law from the perspective of digital evidence and legislatively abolish the Best Evidence Rule and its many exceptions. The rule would then be replaced with legislative provisions which contain a comprehensive list of ways in which a party may adduce evidence of the contents of a document. This would add clarity to the area and would present a positive statutory affirmation of current practices. As it is, the courts operate a discretionary ad hoc approach and admit evidence where to otherwise exclude it on the basis of form alone would work contrary to the interests of justice. The Commission will shortly discusse the Best Evidence Rule in its application to electronic and automated documentary evidence.

(3) Arguments in favour of removing the Best Evidence Rule

2.36 The need to retain the Best Evidence Rule has been critically questioned in several jurisdictions. It has been argued that its failure to make allowances for modern technological advancements as well as the dramatic shifts in the manner in which we now collate, generate and store data have reduced any impact the Best Evidence Rule once had and that its impact is now relatively limited. This coupled with the glut of exceptions to an otherwise exclusionary approach to admitting documentary evidence means that were the rule to be removed this would merely codify a standard which in practice already applies and has been gaining judicial acceptance in other jurisdictions and now in Ireland.

2.37 The issue has been addressed by other law reform agencies. The Queensland (Australia) Law Reform Commission in its 1987 Report on Evidence (which formed the basis for the introduction of the *Evidence Act 1995* (Cth)) concluded that when attempting to prove the contents of a document the Best Evidence Rule was inflexible and ill-suited to the modern means of admitting documents. It noted that:

> "The application of common law rules has given rise to a number of difficulties in proving the contents of writings contained in modern photocopies and microfilm…"[17]

(4) The Current Position of the Best Evidence Rule in Ireland

2.38 In the context of criminal proceedings only, the Oireachtas abolished the Best Evidence Rule in section 30 of the *Criminal Evidence Act 1992* which states:

> "(1) Where information contained in a document is admissible in evidence in criminal proceedings, the information may be given in evidence, whether or not the document is still in existence, by producing a copy of the document, or of the material part of it, authenticated in such manner as the court may approve.
>
> (2) It is immaterial for the purposes of subsection (1) how many removes there are between the copy and the original, or by what means (which may include facsimile transmission) the copy produced or any intermediate copy was made."

2.39 The Best Evidence Rule still applies, at least in principle, in civil proceedings. In *Hussey v Twomey*,[18] discussed below,[19] the Supreme Court has indicated, however, that the Irish courts are likely to follow the approach taken in other States and consign it to history. This followed an earlier judicial discussion on the application of the rule in civil cases in England where it has been argued that it has no standing and may no longer exist. Parker LJ noted in *Masquerade Music v Springsteen*[20] "(i)n my judgment, the time has come when it can be said with confidence that the Best Evidence Rule, long since on its deathbed, finally expired".

2.40 Despite these judicial comments, there remains a prominent vestige of the Best Evidence Rule in Irish law which requires the production of primary

---

17 Available at www.qlrc.qld.gov.au.

18 [2009] 1 ILRM 321.

19 See below paragraph 2.48.

20 [2001] EWCA Civ 563.

evidence of documents. This Primary Evidence Rule operates by requiring that the contents of a document be proved by production of the original and is in essence a modern restatement of the Best Evidence Rule. This was acknowledged by O'Flaherty J in the Supreme Court in 1997 in *Primor Plc v Stokes*[21] where he stated:

> "The Best Evidence Rule operates in this sphere to the extent that the party seeking to rely on the contents of a document must adduce primary evidence of those contents...The contents of a document may be proved by secondary evidence if the original has been destroyed or cannot be found after due search. Similarly, such contents can be proved by secondary evidence if production of the original is physically or legally impossible".

2.41 Prior to the *Primor* case, some relaxation of the strict application of the Best Evidence Rule included the decision in *Martin v Quinn*[22] which involved a drink-driving conviction under section 13(3)(a) of the *Road Traffic (Amendment) Act 1978*. Here it was necessary to prove that the person for whom the defendant had failed to provide a specimen of his urine was a registered medical practitioner. The Supreme Court held that the testimony of that person that he was such a practitioner at the relevant time was *prima facie* evidence of that fact and, unless rebutted, would support a conviction.

2.42 This finding constituted an acceptance by the Supreme Court that some moderation was required and acceptable to mitigate the strict application of the Best Evidence principle, which would otherwise "give rise to the intolerable burden of having to produce formal proof of qualifications held by professional witnesses on every occasion when they were called on to give evidence."[23] The Supreme Court, however, was clear that an appropriate form of *prima facie* evidence must still be furnished, which in the *Quinn* case would have been satisfied by the medical practitioner himself confirming by means of his oral testimony, that he was a registered medical practitioner "at the material time."[24]

2.43 The Supreme Court also drew attention to the discussion in the leading English textbook, *Phipson on Evidence* and the extent to which the English courts had withdrawn from the strictness of the Best Evidence Rule. In doing so, the Court noted that the "actual decisions of the courts show that by

---

21 [1996] 2 IR 459, 518.

22 [1980] IR 244.

23 O Hanlon J in *DPP v O'Donoghue* [1991] 1 IR 448.

24 Henchy J [1980] IR 244, at p 250.

far the most conspicuous feature of the modern law of evidence has been its persistent rescission from the 'best evidence' principle".[25]

2.44 A note of caution was expressed by O'Hanlon J in *DPP v O'Donoghue*[26] when he stated: "I do not think the prosecution can ask for the rule of evidence to be further relaxed, when its compliance can be ensured by this simple expedient."

2.45 *Primor* was approved in 2007 in *Fitzpatrick v DPP*[27] which involved the failure of the prosecution to produce or account for a statement produced by an intoxyliser machine pursuant to section 17(2) of the *Road Traffic Act 1994*.[28] The intoxyliser machine produced two identical statements each giving a reading of 41 micrograms of alcohol per 100ml of breath following which the applicant was duly charged with drunken driving. However when the matter arose in the District Court the prosecution did not put in evidence a statement prepared under s 17 of the 1994 Act. Instead evidence was given of the content by means of a statement produced by the intoxyliser machine. The judge of the District Court rejected the appellant's contention that the original statement was an essential proof in a prosecution for drink driving following which the appellant received a fine and a disqualification from driving. The issue then became whether, in order to secure the conviction of a person accused of drink–driving, a statement prepared under s 17 of the 1994 Act had to be adduced into evidence at all.

2.46 The prosecution wished to adduce evidence to prove the content of a statement produced by a machine under s 17 without producing the statement itself. Under the Best Evidence Rule they would not be permitted to give

---

25 The Supreme Court cited *Phipson on Evidence*, 12th edition (Sweet & Maxwell, 1976), para 128. The most recent edition, *Phipson on Evidence*, 16th edition (Sweet & Maxwell, 2005, with 2 Supplements), confirms the views in the 12th edition.

26 [1991] 1 IR 448.

27 [2007] IEHC 383.

28 Section 21 of the *Road Traffic Act 1994*, provides: (1) A duly completed statement purporting to have been supplied under section 17, shall, until the contrary is shown, be sufficient evidence in any proceedings under the Road Traffic Acts, 1961 to 1994, of the facts stated therein, without proof of any signature on it or that the signatory was the proper person to sign it, and shall, until the contrary is shown, be sufficient evidence of compliance by the member of the Garda Siochana concerned with the requirements imposed on him by or under this Part prior to and in connection with the supply by him pursuant to section 17 (2) of such a statement."

secondary evidence of the content of that statement unless it was first established to the satisfaction of the court that the original statement had been lost or destroyed or could not be presented through impossibility.

2.47 Where no explanation was offered for the absence of the original statement produced by the intoxyliser machine or of the need to rely upon oral evidence as to the content of the statement, secondary oral evidence as to the content of the statement was inadmissible. Secondary evidence of the content of that statement could not be admitted so as to justify the conviction save where it had been first established by evidence that the original statement was lost, destroyed or physically or legally impossible to produce and so the appeal was successful. The court did allow however, that had the prosecution sought to rely on a copy of the original, this could have been done under section 30 of the *Criminal Evidence Act 1992*.[29] Had this section been relied upon it would not have been necessary to prove that the original had been lost or destroyed or that its production was otherwise impossible.

2.48 In *Hussey v Twomey*[30] the Supreme Court has indicated that the Best Evidence Rule can no longer be regarded as part of Irish law in civil proceedings. The case related to whether the best available evidence had to be adduced in a case or whether the prosecution had a degree of choice and discretion when it came to presenting its case.

2.49 The plaintiff had been injured in a traffic accident when she was a passenger in a car driven by one of the defendants. A key issue was whether she had been contributory negligent by allowing herself to be driven in the car at a time when she should have known that the driver was intoxicated. She asserted in her testimony that she had not seen him drinking alcohol and would not have allowed herself to be driven by a person who was intoxicated. The other key evidence in the High Court had been given by the Garda who had come across the scene of the accident. The Garda, who had wide experience of observing intoxicated persons, gave evidence that the driver was visibly intoxicated because his speech was slurred.

2.50 The defendants in this civil claim argued that the best available evidence which could have been adduced in the circumstances was the oral and observational evidence from Garda officers and medical practitioners as to the state of relative intoxication of the driver. In terms of documentary evidence, the plain tiff pointed out that the medical records of the hospital had not been produced. The defendants argued that there was no longer any Best Evidence Rule applicable in these proceedings. As indicated, the Supreme Court agreed

---

29 See paragraph 2.38 above.

30 [2009] IESC 1, [2009] 1 ILRM 321.

with this general approach. While it did not strictly relate to documentary evidence, the rhetoric of the court is useful in forwarding the position that the Best Evidence Rule is no longer tenable in either civil or criminal proceedings.

2.51 Delivering the judgment of the Supreme Court, Kearns J commented on the specific circumstances of the case itself but also made important general statements on the virtual demise of the Best Evidence Rule. It is notable too that rather than artificially imposing a strict adherence to admissibility, but, rather, adhering to the traditional approach of the law of evidence, Kearns J reiterated that admissibility should, ultimately, have an element of "common sense" attached to it.

2.52 In addition to commenting on the specific circumstances of the case, Kearns J went on to indicate clearly that the Best Evidence Rule is no longer part of the law of evidence in Ireland. Kearns J cited with approval a number of comments expressed in the 1982 edition of the leading English textbook, *Phipson on Evidence.*[31] *Phipson* had noted that the English (Divisional) High Court in *Kajala v Noble*[32] had described the Best Evidence Rule as having "gone by the board long ago". This has been reinforced in subsequent English case law. For example, in the English Court of Appeal in *Masquerade Music v Springsteen*[33] Parker LJ commented that: "[i]n my judgment, the time has come when it can be said with confidence that the best evidence rule, long on its deathbed, has finally expired".

2.53 On this basis, Kearns J commented in an important passage of general application:[34]

> "I am thus satisfied it is open to a defendant to make out a case to the required standard either through cross-examination of a plaintiff, circumstantial evidence or indeed any other form of admissible evidence."

2.54 In conclusion, the Commission notes that the general and specific comments made by the Supreme Court in *Hussey v Twomey*[35] reinforce the

---

31 The Supreme Court cited *Phipson on Evidence*, 13th edition (Sweet & Maxwell, 1982), pp.69-73. The most recent edition, *Phipson on Evidence*, 16th edition (Sweet & Maxwell, 2005, with 2 Supplements), confirms the views in the 13th edition.

32 (1982) 75 Cr App R 149 at 152. See paragraph 2.80, below

33 [2001] EWCA Civ 563, at paragraph 84.

34 [2009] 1 ILRM 321, at 14.

35 [2009] IESC 1, [2009] 1 ILRM 321

view that the Best Evidence Rule, as originally understood, no longer forms part of the law of evidence in Ireland. In that respect, the Commission considers that any new statutory framework for the law of evidence should concur with the view approved by the Supreme Court that it has "long gone by the board."

(5) Admitting a Copy under the Best Evidence Rule

2.55 Where an original document is available this must be produced under the Best Evidence Rule as it currently stands. In these instances secondary or derivative evidence will not suffice. In the English case *Forbes v Samuel,*[36] it was decided, however, that where duplicates are available and have been signed by each of the parties, each duplicate is considered an original for the purposes of the rule. In the early 19th century English case *Roe d. West v Davis*[37] it was decided that where the document is a counterpart, it will be treated as an original against the party who signed it. An enrolled copy indicating a private document that has been officially filed in a public office or court (a typical example being a probate copy of a will) will also be treated as an original by the court. Furthermore, in *Attorney General v Kyle*[38] an informal admission by a litigant concerning the contents of a document will constitute primary evidence against that party.

2.56 The purpose of the Primary Evidence Rule was undoubtedly the detection and prevention of fraudulent manipulation of copies or primary documents. It can be argued equally that with the advent of technological advancements the original purpose of the rule has been negated or on the other hand, that it is more relevant than ever before. This is especially because of the ease with which computer documents may be tampered with and fabricated in a manner that could lead to the possibility of such tampered evidence being presented as an unaltered original in the absence of sufficient verification technologies.

2.57 Where evidence falls within one of the exceptions, secondary evidence may be presented by a party attempting to comply with the Best Evidence Rule. This generally takes the form of a copy of the document in issue and this secondary evidence may only be used if proof is available which shows that the writing is an original or duplicate or if an adequate excuse is presented explaining the proponent's non-production of the original. Even in the early 19th century English case *Doe Gilbert v Ross*[39] it was held that there are "no

---

36 [1913] 3 KB 706.

37 *Roe d. West v Davis*, 7 East 363, 103 Eng Rep 140 (KB 1806).

38 [1933] IR 15.

39 (1840) 7 M & W 102.

degrees of secondary evidence" and this approach was legislatively endorsed in section 30(2) of the *Criminal Evidence Act 1992* and so therefore it is of no consequence if the document is a copy of a copy (a derivative) once the secondary evidence rule is engaged.

2.58 In the United States, the Advisory Committee on Proposed Rules to amend the Federal Rules of Evidence noted that the Best Evidence Rule, as a precursor to the secondary evidence rule, had developed as a "rule of preference" and that based on this reasoning, the non-production of an original was not fatal to the admission of a document which as a copy was a representation of the information. This is reflective of the principle of preference, and places different strains of documentary evidence into a hierarchy of preference. This does not accord, however, with the accepted view of documentary evidence that there are no degrees of secondary evidence.[40]

2.59 Although in most cases identifying the original of a document will not prove problematic, this may increasingly feature in litigation in the future, particularly in the wake of changing perceptions of the definition of a document (meaning a primary document). For the purposes of this discussion, the Commission assumes that the definition should now include electronic records, as provisionally recommended in Chapter 1.[41]

2.60 The onset and expanded use of electronic evidence reinforces the need to review the continued utility of the Best Evidence Rule. If the purpose of the Best Evidence Rule is to prevent fraud, it is questionable whether it is sufficiently suited to this task. There are situations in which the rule is inapplicable yet if the intention is the detection and prevention of fraud then it also ought to apply to these other situations.

2.61 In fact, the Oireachtas has taken a different view. In the context of criminal proceedings, section 30 of the *Criminal Evidence Act 1992* removed the requirement to present the original document in criminal proceedings. In the context of a specific form of civil proceedings, section 26 of the *Children Act 1997* applied the same approach to cases addressing the welfare of children. It is clear, therefore, that in Ireland legislation has been enacted which shifts the approach from exclusionary to inclusionary when it comes to admitting documentary evidence. The Commission notes that, consistently with the approach taken by the Supreme Court in *Hussey v Twomey,*[42] discussed above, if a more inclusionary approach is taken this would lead to a shift towards assessing the weight to be apportioned to the evidence in question.

---

40 Available at www.access.gpo.gov/uscode/title28a.

41 See above paragraph 1.33.

42 [2009] IESC 1, [2009] 1 ILRM 321

(6) The Applicability of the Best Evidence Rule to Electronic and Automated Documents in Ireland

2.62 The Commission now turns to examine specifically how the best evidence rule applies to documentary evidence emanating from a mechanical or electronic device. As already discussed in Chapter 1, the term 'document' has been interpreted widely at common law and would seem to encompass electronic records, and the Commission has provisionally recommended that a technology-neutral approach should be taken in any proposed statutory framework on documentary evidence.[43]

2.63 As discussed above, should an adducing party seek to rely on the contents of a document, the Best Evidence Rule requires the production of the original document as a default. This original as produced must then be accompanied by oral explanatory testimony through which to establish that the document is indeed what the adducing party claims it to be.

2.64 Digital "device-based" evidence is, in its truest form, rarely in a format readable by humans. As such, another step is required for admitting any electronic or automated document into evidence. Conceptually, any additional step creates a new document, which might otherwise not qualify under the Best Evidence Rule if strictly applied.

2.65 Computer printouts, however, are a form of primary reproduction of otherwise illegible and unquantifiable documentary data held in a latent image and which, in the absence of a printout, has no physical counterpart.

(a) Electronic and Automated Documentary Evidence Explained

2.66 The filing of records electronically includes the steps involved in storing computer processed information in storage media. These can involve magnetic disks or tapes, where the data is represented in the form of machine readable codes or patterns imprinted on magnetisable surfaces by electronic impulses.

2.67 The use of computer drives and systems to store data and documentation is one of the most distinctive advantages of information technology systems encompassing both the rendition and archiving of data. This saves on labour and storage costs and serves to expedite document searches and retrieval both on-site and remotely when accessed via a computer network. The Best Evidence Rule evolved long before computer technology had developed. It evolved at a time when it was still possible for human visual observation alone to compare accurately an original with the proffered copy. With the emerging recognition of the differences between paper and electronic

---

[43] See paragraph 1.36.

documentation, it is now acknowledged that it is not possible by human visual observation alone to compare a hard-drive original with a printer-derived copy.

2.68 Electronic devices which produce images independent of human agency and which record these data through technology alone provide no true tangible original that could be produced in evidence. Thus any printed or displayed image created from the primary representation of data is a copy. The image available for reproduction in evidence is a copy of the first, possibly temporary, recording stored in the device's memory, which is admissible as evidence. As already mentioned (and discussed in more detail in Chapter 3 below), the evidential weight to be given to this will depend on its being properly authenticated.

(b) Video Recordings as Documentary Evidence

2.69 This does not, however, dispose of the question as to the operation of the Best or Original Evidence Rule in relation to the admissibility of an electronic record. This question was noted by Dawson J in the Australian case *Butera v DPP for the State of Victoria*[44] in relation to a specific type of electronic record; an audiotape, although it could equally be asked of other types of electronic records. *Butera* is, therefore, a good place to begin an examination of the principles applying to the refusal to extend the rule excluding derivative evidence to physical objects, a course which is now being followed in Ireland.

2.70 The matter of what will satisfy the court to ensure the admissibility of an electronic record is a question of increasing importance as new technologies emerge. Unlike paper documents whose contents are readily apparent (despite the possible inconvenience involved in producing the original in court), electronic records commonly rely on some other mechanical device to reproduce the data that is held within them.

2.71 In *Butera* the accused had been convicted of conspiring to traffic in heroin. Part of the evidence against him included an audiotape recording of a conversation of the four co-conspirators throughout the course of which the accused was referred to several times. The conversations were conducted in English, Punjabi, Thai and Malay and therefore the tape had been translated into English and was presented as a transcript for the proceedings. The court in *Butera* laid down the following rules regarding the admissibility of audiotape recordings:

- An audiotape recording is not by itself admissible evidence of what is recorded on it. It is the sounds that are produced when the audiotape is played in court that are the evidence admitted to prove what is recorded;

---

44 (1987) 146 CLR 180.

- When an audiotape recording is available, or its absence is not accounted for satisfactorily, the contents of the recording can be proved only by playing the recording in court;
- If an audiotape recording is not available and its absence has been accounted for satisfactorily, secondary evidence of its contents may be given by a witness who heard it played over, or by the receipt of a transcript of the recording; and
- The secondary evidence rule does not exclude evidence derived from an audiotape recording that has been mechanically or electronically copied from an original audiotape recording. Provided the provenance of the original recording, the accuracy of the recording process and the provenance of the copy audiotape recording are satisfactorily proved, there is no reason why the copy audiotape recording cannot be played over in court to prove the contents of the original recording.

2.72 In *Butera* the following observation was made in relation to the admissibility of an audiotape:

> "A tape is not by itself an admissible object for by itself it is incapable of proving what is recorded on it: it is admissible only because it is capable of being used to prove what is recorded on it by being played over. By using sound reproduction equipment to play over the tape, the court obtains evidence of the conversation or other sound which is to be proved; it is that evidence, aurally received, which is admissible to prove the relevant fact." [45]

2.73 This aspect of electronic records recognises the difficulty in identifying what the original of an electronic record is as opposed to what are merely copies. This is a task more uncertain than any encountered when dealing with paper documents. To satisfy the Best Evidence Rule, is a computer file that exists on a hard disk an 'original' document? If so, is a computer printout of that file a 'copy' of that document?

2.74 Evidence in the form of a tape recording is capable of having the characteristics of a document in that it can be reproduced before the court in permanent legible form, as provided for in section 2 of the *Criminal Evidence Act 1992.* It is equally capable of being admitted as a document in line with the Commission's provisionally recommended definition of a document as "anything in which information of any description is recorded".[46] This means that a tape recording remains admissible as documentary evidence. It is logical then that

---

[45] (1987) 164 CLR 180 at 190, Mason CJ, Brennan and Deane JJ.

[46] See paragraph 1.33.

this “document” can be admitted as evidence and raises questions as to how this can be proven in evidence. Can its contents be proved only by the production of the original tape or can it be proved by means of a copy, either in the form of another tape or in the form of a transcript? Under the Best Evidence Rule as applying to written documents, a document must be proved by the production of the original document itself and not by secondary evidence of its contents unless the absence of the original is accounted for and excused.

2.75 While *Butera* was concerned with the admissibility of a transcript of a tape-recorded conversation, rather than with the admissibility of a copy of a tape recording, the court suggested that a copy of a tape recording would be admissible as evidence of the contents of the original recording[47]:

> “It is desirable to add, however, that the best evidence rule is not applicable to exclude evidence derived from tapes which are mechanically or electronically copied from an original tape. Provided the provenance of the original tape, the accuracy of the copying process and the provenance of the copy tape are satisfactorily proved, there is no reason why the copy tape should not be played over in court to produce admissible evidence of the conversation or sounds originally recorded. There is no reason to apply the best evidence rule to copy tapes…”

2.76 Under this approach, therefore, transcripts may be admitted as real evidence, independent of witness testimony and subject only to the admissibility of the recording of which they are a transcript. This is so that any discrepancies which could have passed unnoticed are detectable for example where the document is a transcript of a tape recording in a different language or of bad quality. The standard the tape must achieve is not absolute however and it is not necessary for the party tendering the tapes to show irrefutably that they are accurate.[48]

2.77 In the later Australian case *R v Chen* it was held that the test is whether there is evidence enough before the court to allow the trier of fact (whether a judge or jury) to conclude that the recorded sounds reproduce those originally made and that there is no blanket requirement for a witness to be called to swear testimony that he or she has heard the tape recordings in full and to swear that they have not been tampered with.[49]

---

47 *Butera v DPP* (1987) 164 CLR 180 at 190.

48 *Butera v DPP* (1987) 164 CLR 180 at 188, *R v Ali* [1966] 1 QB 688.

49 *R v Chen* [1993] 2 VR 139 at 150.

2.78 The High Court of Australia in *Butera* also noted that the transcript is not an independent piece of documentary evidence and that it constitutes documentary hearsay where admitted as to the truth of the conversation it records. Thus, the Court held that a transcript cannot be used to prove whether the recorded conversation took place. It is instead secondary evidence of this conversation and, as the Court concluded in *Butera*, is more suitably seen as an "aid to perception".[50]

(c) The Best Evidence Rule and Video Footage

2.79 The *Butera* case involved a significant development in the way Australian law chose to interpret an "original" for the purposes of the Best Evidence Rule and it represented an expansion of the categories of admissible documentary evidence. Similar approaches have been taken in other States in connection with other documentary materials, particularly electronic, mechanical and technological derivatives.

2.80 We have already noted that, in *Kajala v Noble*[51], the English (Divisional) High Court noted that any notion that the Best Evidence Rule as having always required an original document had "gone by the board long ago." As already discussed, these words were quoted with approval by the Supreme Court in *Hussey v Twomey.*[52] In *Kajala* the defendant had been convicted of a breach of the peace and threatening behaviour, having been identified from a videotape copy of original BBC news footage. His counsel argued that the video was inadmissible given that the original film was located in the BBC archives and should have been produced. He argued that failure to present this was in effect a breach of the Best Evidence Rule but this was rejected by the (Divisional) High Court. Ackner LJ noted that:

> "The old rule, that a party must produce the best evidence that the nature of the case will allow, and that any less good evidence is to be excluded, has gone by the board long ago. The only remaining instance of it is that, if an original document is available in one's hands, one must produce it; that one cannot give secondary evidence by producing a copy. Nowadays we do not confine ourselves to the best evidence. We admit all relevant evidence. The goodness and badness of it goes only to weight, and not to admissibility… In our judgment, the old rule is limited and confined to

---

50 *Butera* at 188.

51 (1982) 75 Cr App R 149.

52 [2009] IESC 1, [2009] 1 ILRM 321. See paragraph 2.48, above.

written documents in the strict sense of the term, and has no relevance to tapes or films."[53]

2.81 The *Kajala* case is a good example of judicial adaptation and intellectual pragmatism as regards the need to take account of new technology. In view of the general approval of this rhetoric by the Supreme Court in *Hussey v Twomey*,[54] the Commission considers that this reflects the approach that would be taken in Irish law. There is good reason to believe, therefore, that the adaptability and intellectual pragmatism indicated in 1982, and approved in 2009 by the Supreme Court, would be sufficiently adaptable to accommodate modern technological advancements which have since occurred and are likely to continue into the future.

2.82 Consistently with the approach of the English courts in *Kajala v Noble* a copy of a recording, where identified as authentic, has been accepted in the Australian courts without any reference to or obligation to produce the original. However where only part of an original is tendered it is unlikely the evidence would be admitted.[55]

2.83 Stills and photographs taken from videos are also acceptable as documentary evidence. In *R v Dodson and Williams*[56] the English Court of Appeal held that a photograph taken by a video camera of a building society was admissible as evidence.

2.84 In *R v Cook (Christopher)*[57] the English Court of Appeal permitted a photofit sketch to be admitted as real evidence. The Court was of the opinion that it was not hearsay and was analogous to a photograph as it was a graphic representation of a witness's memory and was admissible as documentary evidence.

2.85 Video recordings are generally watermarked in each frame which can be individually isolated and can be this examined for authentication purposes.

---

53 Citing *Garton v Hunter* [1969] 1 All ER 451, per Lord Denning M.R. at 453e; see also Archbold, Criminal Pleading, Evidence and Practice (40th ed.), para 1-001.

54 [2009] IESC 1, [2009] 1 ILRM 321. See paragraph 2.48 above.

55 Mead, L. "*Usage of video recordings in surveillance, the value of such as evidence and potential problems which can arise.*" discussing *R v Curran and Torney* [1983] 2 VR 133, 13th Annual BILETA Conference: "*The Changing Jurisdiction*" March 1998. Trinity College, Dublin. Available at http://www.bileta.ac.uk/98papers/mead.html 02/04/2005.

56 [1984] 79 Cr App Rep 220.

57 [1987] QB 417.

This can be undertaken at a superficial visual software programme level to verify that the video recording has not been tampered with.

(7) Discussion and Conclusions

2.86 The exclusionary rules render secondary evidence generally inadmissible to prove the content of a writing. The replacement of the best evidence rule and adoption of a new secondary evidence rule would raise the position of secondary evidence to being statutorily admissible (other than oral testimony) as evidence of proof of itself as a documentary instrument, but could also retain the discretion of the courts to exclude such evidence if a genuine dispute existed as to the material terms of the writing and where justice required its exclusion.

2.87 The courts retain the facility to develop principles and exceptions to accommodate documentary evidence and enable it to overcome the strict application of the Best Evidence Rule including in relation to different types of digital records. However it is arguable that leaving the common law to develop such principles in isolation would lead to uncertainty.

2.88 Technological growth including the dramatic rise in use of fax transmissions, e-mail and other electronic communications pose new complications in applying the Best Evidence Rule and its exceptions. Having evolved from an 18th century principle, the rationale for the rule no longer withstands scrutiny, as the Supreme Court confirmed in *Hussey v Twomey*.[58] Before setting out its provisional recommendations on this in Part D, the Commission discusses in Part C the existing exceptions to the exclusionary approach in Ireland. In Part D, the Commission discusses the fate of the Best Evidence Rule in other States and, after this comparative analysis, sets out its conclusions and provisional recommendations.

C Exceptions to the Exclusionary Rules in Ireland

2.89 The Commission has already noted that there are judicially recognised excusing circumstances where the non-production of an original document is not fatal to having documentary evidence accepted. This was alluded to by O'Flaherty J in *Primor plc v Stokes Kennedy Crowley*[59] where it was acknowledged that "(t)he contents of a document may have to be proven by secondary evidence if the original has been destroyed or cannot be found after due search."

---

58 [2009] IESC 1, [2009] 1 ILRM 321.

59 [1996] 2 IR 459.

2.90 In *Attorney General v Kyle*[60] the High Court held that the previously strict requirement for the production of primary evidence does not apply where the existence or specification of the record, as opposed to the contents, are in issue. It does not, therefore, constitute documentary hearsay.[61]

(1) Loss, Destruction and Impossibility of Production

2.91 In the Supreme Court decision in *McFarlane v DPP and Another*[62] Hardiman J acknowledged that the rules of evidence ought not be static and rigid in application. In making allowances and exceptions for the loss of evidence, he noted that it is:

> "part of ordinary human experience that documents and items, even those of great significance or intrinsic value, are not infrequently lost. The law has taken note of this over many centuries and is not so unrealistic as to consider that the loss of an original document or item of real evidence is fatal to any litigation based on it."

2.92 Hardiman J also acknowledged the practical necessity of receiving derivative evidence in situations where it is neither possible nor practical to produce the actual object. He stated:

> "This may take the form of photographs or films of the object or the oral evidence of someone who has seen it."

2.93 As the High Court of Australia held in the *Butera* case already referred to, the requirement is also dispensed with when the documents in question are in a non-written form such as audio tapes and video recordings.[63]

2.94 In the case of a digital camera, strictly speaking the "original" is the digital file (the binary digits) representing the image stored on a memory chip or storage device such as a disk. This does not pose a problem for criminal proceedings in Ireland because section 2 of the *Criminal Evidence Act 1992* defines a "document" as including information which is brought before the court in the form of a "reproduction in permanent legible form, by a computer or other

---

60 [1933] IR 15.

61 Documentary hearsay is evidence produced in the form of a document which is offered as proof of the statements contained therein as occurred in *Myers v DPP [1965] AC 1001* (see paragraph 2.109 below). The evidence is inadmissible as, as with oral hearsay, the truth of the out of court documentary assertions cannot be tested by cross-examination and may be accepted as having a probative force to which it is not entitled. (*R v Blastand* [1985] 2 All ER 1095).

62 [2006] IESC 11.

63 *Buttera v DPP (Vic)* (1987) 164 CLR 180.

means (including enlarging), of information in non-legible form". This includes information such as digital photographs which would otherwise be unrecognisable in their true form. These reproduced "copies" are, therefore admissible in evidence in criminal proceedings. While there are comparable provisions for civil proceedings, these tend to be niche provisions rather than there being an overarching exception.

(a) Common law exceptions to the requirement to produce original documents

2.95 The main common law exceptions to the requirements to produce an original document are:[64]

(i) Failure to comply with a notice to produce

As Cross explains:

> "A notice to produce informs the party upon whom it is served that that party is required to produce the documents specified therein at the trial to which the notice relates. The notice does not compel production of the documents in question, but the fact that it has been served provides a foundation for the reception of secondary evidence."[65]

2.96 It may happen that the party served with a notice to produce the documentary material fails to produce it. If so the opposing party is entitled to give secondary evidence of the contents of that document. On the other hand if the original document is not in possession of the opposing party, the proper course is to subpoena the party who does have control of the document in an effort to gain access to the information.

(ii) Document lost or Destroyed

2.97 If it is proved, by or on behalf of the person who should be in possession of the document, that it has been searched for without success, secondary evidence of the contents of the document will be admissible. Here the court will accept a copy of the disputed document (or oral evidence as to its existence and content) in situations where the original has been accidentally destroyed or lost as in *R v Thompson.*[66]

---

64 See further Murphy, P. *Murphy on Evidence*, Oxford University Press, 11th Ed, 2009, p 609.

65 The Receipt of Evidence by Queensland Courts: Electronic Records, Issues Paper WP No 52 Queensland Law Reform Commission, August 1998, p 12.

66 [2001] 1 NZLR 129.

2.98 Such a situation often arises in instances where title deeds have been lost or damaged with the passage of time as occurred in *Nally v Nally*[67]. Where a document has been damaged and reconstructed it is solely the person responsible for the reconstruction who can offer secondary evidence as to the contents of the original as can be seen from *People (DPP) v Marley.*[68]

2.99 In the English case *R v Wayte*[69] the Court held that secondary evidence in the form of a photocopy of a document is admissible in place of that document where they are relevant and the original is unavailable through loss or destruction. Beldam J reiterated that "there are no degrees of secondary evidence." He also added that:

> "The mere fact that it is easy to construct a false document by photocopying techniques does not render the photocopy inadmissible. Moreover, it is now well established that any application of the best evidence rule is now confined to cases in which it can be shown that the party has the original and could produce it but does not."[70]

2.100 The passage quoted from the judgment of Beldam J in *R v Wayte* was approved and applied by the Northern Ireland Court of Appeal in *Public Prosecution Service v Duddy*,[71] where the Court held that a copy of a breath test certificate was admissible in a drink driving prosecution where the original had been lost and could not be found after due search. At the defendant's trial on a charge of drink driving, the original certificate of the breath analysis could not be found and was marked down as lost. Counsel for the prosecution then sought to adduce a photocopy of the certificate deposed by the officer who had created the original as an exact photocopy of the document. He also testified that his signature was correct. An application was made to admit these copies as secondary evidence under Article 30 of the *Criminal Justice (Evidence) (Northern Ireland) Order 2004,*[72] the equivalent of section 30 of the *Criminal Evidence Act 1992.* The magistrate exercised his discretion to refuse to admit the evidence on the ground that these copies could not be fully authenticated following the loss of the original as they were "at best poor copies" of

---

67 [1953] IR 19.

68 [1985] ILRM 17.

69 (1982) 76 Cr App R 110.

70 *Ibid,* at 116.

71 [2008] NICA 18.

72 S.I. 2004/1501.

documents lost and sufficient notice had not been given to the respondent to challenge these documents.

2.101 On appeal, the Northern Ireland Court of Appeal held that the documents ought to have been admitted and that there was nothing in the 2004 Order entitling the magistrate to exercise his discretion based on the condition of the documents. This issue would, the Court held, go to weight rather than to admissibility. Delivering the judgment of the Court, Kerr LCJ expressly approved and applied the passage from the judgment of Beldam J in *R v Wayte* already quoted. He added that there was "no sensible reason that evidence from the police officer that the document was an exact copy of that which he had completed should not be sufficient to authenticate it." The appeal was allowed and the court noted that, in circumstances where the document has been lost and where testimony has been offered so as to vouch for the integrity of the copy, the trial court could not properly exercise its discretion to exclude the document from evidence under Article 30 of the 2004 Order.

(iii) Production of Original Impossible

2.102 Where the original is in the hands of an individual outside the jurisdiction so that the person could not be compelled to produce it, secondary evidence of the contents of the document will be admissible. This is likely to occur where a document is physically or legally impossible or very difficult to obtain, as was the case in *Primor plc v Stokes Kennedy Crowley*[73] such as where the opposing party has the original and has failed to turn it over to the proponent.

2.103 In the 2003 English case *Post Office Counters v Mahida*[74] the adducing party sought to admit secondary documentary materials where the originals had been destroyed by that party. This case is noteworthy in that it held that judicial discretion to exclude evidence in civil proceedings also necessarily implied the power to accept copies in the alternative. This extended to accepting copies of documents even where the originals could not be produced owing to the fault of the party seeking to rely on the copies. The secondary evidence was duly admitted but the propounding party failed on grounds of weight as the evidence was not sufficient to prove the amount of the disputed debt in question.

(iv) Production of Original Inconvenient

2.104 For secondary evidence to be permitted it is not necessary for the documents to be factually inaccessible and the court will permit evidence of

---

73 [1996] 2 IR 459.

74 [2003] EWA Civ 1583.

documents to be adduced by secondary materials where it would be highly inconvenient to produce the original of a document in court, as demonstrated above in the case of chalked letters and funereal plaques etc.

2.105 This can also be seen in, for example, the English case *Owner v Bee Hive Spinning Co Ltd*[75] where the document in question was a notice setting out mealtimes and which was required by statute to be affixed to and was so mounted on the wall of a factory. The opposing party may serve a notice to produce the document and failing this resort to secondary evidence.

(v) Public documents[76]

2.106 It has been a long-established part of the law of evidence that the content of a number of types of public documents could be proved by copies of various kinds. This was based on the inconvenience that would be involved in requiring production of the originals.

2.107 The Commission suggests that removing the Best Evidence Rule in its entirely would remove the need to place these various exceptions within the traditional exclusionary approach of the law. This could also be done while maintaining scope for judicial discretion to accommodate new scenarios arising where derivative documentary evidence is sought to be admitted. An inclusionary approach as suggested would consolidate the many common law exceptions and aid judicial interpretation while ensuring coherency and predictability for parties to litigation. Indeed, it is arguable that the many existing inclusionary exceptions indicate a tacit acceptance of the need for further reform.

D The Abolition of the Best Evidence Rule in other jurisdictions

2.108 The Commission now turns to examine the amendments made to the law of evidence in other jurisdictions to accommodate electronic evidence and which has resulted in the main in the abolition of the Best Evidence Rule.

(1) The Best Evidence Rule in England

2.109 In *Myers v Director of Public Prosecutions*[77] the defendant had been charged with receiving stolen cars. The prosecution tendered records of the car manufacturer as evidence of identity of some of the cars. The House of Lords held that the records were not admissible because the numbers entered

---

75 *Owner v Bee Hive Spinning Co Ltd* [1914] KB 105.

76 For a further fuller discussion on public documents as admissible evidence see Chapter 3.

77 [1965] AC 1001.

upon them were merely "assertions by the unidentifiable men who made them that they had entered numbers they had seen on the cars." The Court was not prepared to create a new exception to the hearsay rule to cover this type of situation. The Law Lords emphasised, indeed, that reform of the hearsay rule was more appropriately dealt with by legislation. Lord Reid commented:

> "If we are to extend the law it must be by the development and application of fundamental principles. We cannot introduce arbitrary conditions or limitations; that must be left to legislation: and if we do in effect change the law, we ought in my opinion only to do that in cases where our decision will produce some finality or certainty. If we disregard technicalities in this case and seek to apply principle and common sense, there are a number of parts of the existing law of hearsay susceptible of similar treatment... The only satisfactory solution is by legislation following on a wide survey of the whole field."

The English *Criminal Evidence Act 1965* was enacted specifically to reverse the effect of the *Myers* decision. As for civil proceedings, the Best Evidence Rule was in effect abolished by sections 8 and 14 of the *Civil Evidence Act 1995*[78] which permit proof by secondary evidence. Section 8 of the *Civil Evidence Act 1995* outlines the means of proving documents for admissibility in civil proceedings.

2.110 In 2008 *Blackstones Criminal Practice* recognised that:

> "The best evidence rule, which was used in the 18th and early 19th centuries as an exclusionary principle, ie to prevent the admission of certain evidence where better evidence was available, is now all but defunct."[79]

2.111 Of note also is Lord Denning MR's comment in *Garton v Hunter* that

> "The old rule, that a party must produce the best evidence that the nature of the case will allow, and that any less good evidence is to be

---

78 Section 8- of the 1995 Act states:"(1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved— (a) by the production of that document, or (b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the court may approve. (2) It is immaterial for this purpose how many removes there are between a copy and the original. Section 14 of the 1995 Act also preserved the older statutory provisions relating to public documents.

79 Hooper, Ormerod, Murphy and Ors, *Blackstone's Criminal Practice* (Oxford, 2008), at 2285.

excluded, has gone by the board long ago. The only remaining instance of it is that, if an original document is available on one's hands, one must produce it; that one cannot give secondary evidence by producing a copy. Nowadays we do not confine ourselves to the best evidence. We admit all relevant evidence. The goodness or badness of it goes only to weight, and not to admissibility".[80]

(a) The Status of Electronic Documents in Satisfaction of the Best Evidence Rule.

2.112 Whether the court would approach documents stored by imaging and scanning on computer as a document in writing, or analogous to a photograph, is now a moot point in the UK. Section 10 (d) of the *Civil Evidence Act 1968* provides that any "device in which one or more visual images are embodied" are included which appears to cast the net sufficiently wide to cover the possibility of electronic documents.

2.113 The admissibility of statements produced by computer is provided for in section 5 of the 1968 Act, as amended by the *Civil Evidence Act 1995*, which also contains the definition of a computer.

> "(1) In any civil proceedings a statement contained in a document produced by a computer shall, subject to the rules of court, be admissible as evidence of any fact stated therein of which direct evidence would be admissible, if it is shown that the conditions mentioned in subsection (2) below are satisfied in relation to the statement and computer in question.
>
> (2) The said conditions are –
>
> that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store and process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by any body, whether corporate or not, or by any individual;
>
> that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;
>
> (c) that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that

[80] *Garton v Hunter* [1969] 1 All ER 451, [1969] 2 QB 37.

period was not such as to affect the production of the document or the accuracy of its contents; and

that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities."

2.114 The effect of this section was to permit the reception of what would otherwise constitute hearsay statements, including second-hand hearsay statements, contained in computer-produced documents avoiding the need for the formalities of the Best Evidence Rule and thereby effectively statutorily bypassing the application of the Rule.[81]

2.115 The *Civil Evidence Act 1968* also enacted various sections the effect of which meant that "computer" also covered any combination of computers, or different apparatus operating in succession over the period in question thereby offering a solution to any difficulty which may have been encountered by the transfer of the "imaged" documentary data from one computer to another. The number of transfers was deemed immaterial to the admissibility of the information.[82]

2.116 In 1993 the English Law Commission examined the law of England and Wales relating to admissibility of hearsay evidence in civil proceedings and considered whether the rule against hearsay (as modified by the Civil *Evidence Acts*) should be retained and if so to what extent.[83] The Law Commission recommended that the rule against hearsay evidence should be abolished. The general view was that of a prevailing unwieldy statutory regime where the law was unnecessarily ambiguous, difficult to understand and in some instances outmoded and that the rules governing its practical application were too complicated.

2.117 The Law Commission concluded that developments in the law had overtaken the Best Evidence Rule. Insufficient recognition was taken of the modern practice of civil litigation which had been adapted to focus emphasis on ensuring that, subject to considerations of reliability and weight, all relevant evidence is capable of being adduced in evidence. This blunted the severity of the Best Evidence Rule which previously saw relevant evidence excluded for the sake of conformity with the law. This was also influenced by a climate promoting pre-trial discovery with more emphasis on identifying and refining the issues in advance which in turn lessened the opportunity parties may otherwise

---

81 *Civil Evidence Act 1995* Section 5(6).

82 Section 5(3).

83 *The Hearsay Rule in Civil Proceedings* (Law Com No 216, 1993)

have taken advantage of raising technical points at the trial stage. The English *Civil Evidence Act 1995* was enacted on foot of the Law Commission's recommendations.

(b) Civil Evidence Act 1995

2.118 Section 1 of the 1995 Act provides:

> (1) In civil proceedings evidence shall not be excluded on the ground that it is hearsay.
>
> (2) In this Act -
>
> (a) 'hearsay' means a statement made otherwise than by a person while giving oral evidence in the proceedings in which it is tendered as evidence of the matters stated; and
>
> (b) references to hearsay include hearsay of whatever degree.

2.119 Sections 2 to 5 go on to establish various safeguards in relation to the admissibility of hearsay evidence, such as requiring the party proposing to adduce such evidence to give notice to the other party to the proceedings. Section 2 grants the opposing parties the power to call the person who made the hearsay statement and cross examine him although he may not have been called by the proponent.[84] Section 4 sets out five factors to be taken into account by the Court in assessing the weight to be given to the hearsay evidence adduced and states that hearsay evidence shall not be admitted if at the time it was made the maker was not competent to execute such a statement.

2.120 A number of specific sections were introduced to satisfy the need to adduce computer and electronically generated documents and data without contravening the spirit of the Best Evidence Rule. Of direct relevance to the question of the admissibility of computer generated/stored records set out above is section 8 dealing generally with the proof of computer outputs and providing that proof of statements contained in documents:

> (1) where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved -
>
> (a) by the production of that document, or
>
> (b) whether or not the document is still in existence, by the
>
> production of a copy of that document or of the material part of it, authenticated in such manner as the court may approve.

---

[84] *Civil Evidence Act 1995,* Section 3.

(2) It is immaterial for this purpose how many removes there are between a copy and the original.[85]

2.121 The *Civil Evidence Act 1995* thus removed the difficulties associated with the Best Evidence Rule and admissibility of documents "scanned" into a computer and then reproduced, giving the Court discretion to determine the appropriate test for authentication of the document in the circumstances of each case.

(2) Australia

2.122 The Australian Law Reform Commission recommended a new regime to address the system by which to judge the proof of the contents of a document as sufficient and admissible. This was subsequently translated into in Part 2.2 of the *Evidence Act 1995* (Cth) which replaced most of the common law and varying State and Territory statute law on evidence, replacing it with a single unified legislative enactment reforming the federal justice system. The *Evidence Act 1995* effectively abolished the Best Evidence Rule altogether. This legislative regime now no longer requires an original of a document to be tendered in preference to a copy. In fact, throughout the *Evidence Act 1995* (Cth) there has been a seemingly deliberate effort to avoid any reference to an "original" document thus obviating the need to determine which format of a document is the original and which is merely a derivative with section 47 containing definitions and section 48 addressing the proof of contents of documents.

2.123 The uniform Australian *Evidence Act 1995* makes ample allowance for the admissibility of electronic and automated evidence with provisions which permit secondary evidence and dissolve the stringencies of the Best Evidence Rule.

2.124 Section 48 of the Australian *Evidence Act 1995* outlines the manner in which the contents of a document can be proved. As well as tendering the original document itself, the contents may be adduced and proven by testimony of a party to the proceedings as to its contents,[86] or indeed by tendering a copy

---

85 In regard to these provisions, section 13 contains the following definitions:

"document" means anything in which information of any description is recorded, and "copy" in relation to a document, means anything on to which information recorded in the document has been copied, by whatever means and whether directly or indirectly; "statement" means any representation of fact or opinion, however made."

86 See the Uniform *Evidence Acts 1995* s48 (1)(a), although such an admission can only be used against the party who made the admission or who adduced evidence of it (s48 (3)).

of the document which need not be an exact copy so long as it is "identical in all respects".[87]

2.125 Also, where the impugned document is an article or thing that records sounds, or in which words are recorded as code (eg short-hand writing), the contents can be proved by tendering a transcript of the recording or decoded words. The contents can also be validated by tendering a document produced by a device to retrieve stored information,[88] by tendering a copy of a public document where printed by the Government Printer or by the authority of same or by or on behalf of a foreign government.[89]

2.126 To this end the Uniform Evidence Acts define the concept of a "public document" in section 48 (1)(f) as a medium of information retention that forms part of the records of, or is being kept by or on behalf of the Crown, a foreign government, a person or body holding office or exercising a function under the constitution of an Australian or foreign law.

2.127 If the document is deemed "unavailable"[90] or where neither the existence nor the contents of the document are being disputed, it may still be adduced by tendering a copy, summary or extract or, failing that, by adducing oral evidence of its contents.

2.128 In updated territorial Evidence Acts, for example, the Victorian *Evidence Act 2008,* it is provided that audio and televisual recordings fall within the elastic confines of the term "document". They are also a species of real evidence as the court is able to view them firsthand and then interpret the recorded information presented to them. The Uniform Evidence Acts in many ways comprises a more exhaustive legislative regime; a one stop shop adjudicating on documentary evidence.

(3) Authentication and the Best Evidence Rule- Australia

2.129 A document for the purposes of the *Evidence Act 1995* and integrated into individual State law most recently by the Victorian *Evidence Act*

---

87 Section 48 (1)(b).

88 Section 48 (1)(d).

89 Section 48 (1)(f).

90 Such a situation would be deemed to arise where the document cannot be found after reasonable search and inquiry, where it has been destroyed otherwise than in bad faith, where it would be impractical to produce it, where its production would expose the producing party to prosecution, where it is without the party's possession or control and can be reached neither by judicial procedure of the court nor under the control of any party to the proceedings.

1995, includes any medium from which sounds, images or writings can be reproduced. This potentially includes every type of data storage medium in the computing and electronic communication gambit for example a hard drive, a floppy disk, a tape drive and a compact disk.

2.130 Section 48(1)(b) provides that the contents of a document may be adduced in evidence by tendering the document itself or a copy thereof which has been produced by means of "a device that reproduces the contents of documents" and which can be taken to include a photocopy machine or, given the very wide definition of document, a computer which reproduces the contents of a hard drive by retrieving the relevant data and sending it to a printing device.

2.131 The particular technology represented by a personal computer is covered in more detail in section 48(1)(d). This states that, if the document comprises a thing in which information is stored and is not legible unless a device is used to retrieve it, the information can be introduced by tendering a document that was, or purports to have been, produced by use of that device. It would seem that either section 48(1)(b) or section 48(1)(d) could be relied upon to introduce computer printouts subject only to formal proof that they issued from a printer as a result of an instruction given via the appropriate software.

2.132 Sections 146 and 147 facilitate the authentication of documents which are tendered by a party who asserts that they reflect the results of a process performed by a computing device. They relate to establishing the "proper custody" of the document and its provenance. They concentrate on the facilitation of proof.

2.133 Section 146 provides that the product of the particular process is properly reflected in the document and aims to establish that the process used is one that, if properly used, ordinarily produces that same outcome. Therefore it would not be necessary as this would use time and resources, to call evidence to prove that a photocopier normally produced complete copies of documents and that it was working properly when it was used to photocopy a particular document. This sets up a rebuttable presumption that the process used has accurately and faithfully copied the document.

2.134 Section 147 deals with documents shown to have been produced by processes, machines and other devices as part of the records for the purposes of carrying on a business. The same inference of accurate and reliable operation will be drawn provided the document was produced by the particular technological endeavour in use at the time for the purposes of the business. In the case of business records, therefore, there is no need to make out a prima facie case that the process by which they were created was in fact reliable. Instead "it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document on the occasion in

question, the device or process produced that outcome" thereby effectively allowing a lower operational threshold.

(4) The US Perspective: the Exclusionary Rules of Evidence in Relation to Electronically Stored or Generated Documents

2.135 In the US legislative code precautions have been taken to assure the admissibility and probative value of electronic documents. The path taken has been one of prescription and the benchmarking of electronic documents as against their paper counterparts.

2.136 Presently the rules of evidence are not vastly different for electronically stored documents than for their paper counterparts. However, because electronic files are seen and depicted as particularly susceptible to purposeful or accidental alteration and incorrect processing, laying a foundation for their admission must be done with particular care. The standard which this foundation must achieve will be discussed in Chapter 5 in its focus on admissibility and authentication of electronic and automated documentary evidence.

(a) Retrieving or Generating "an Original" from an Electronic Format in the US

2.137 Electronic files[91] are dubbed "machine readable" because they can be copied into a computer for processing and interpreted for printing out in human readable form be it on paper or microfilm, or on a video display screen. Issues arise in the production of an original in satisfaction of the Best Evidence Rule as well as in an effort to avoid falling foul of the Hearsay Rule. In accordance with the Best Evidence Rule an "original" of a record is the record itself, which can pose a problem regarding computer printouts where the system delineates between paper and electronic and automated documentary evidence. Where rigidly applied, this rule serves to preclude the admissibility of anything but the original document to prove its content. In a comprehensive, forward thinking move, acknowledging the impracticality of this rule when applied to magnetic files, many US states (and the Federal government) moved to adopt rules that define and label computer printouts as original, provided that they are shown to accurately reflect the information contained therein.

2.138 Even in the absence of such a rule, incidences have taken place where computer printouts of records stored in magnetic media have been raised to the status of original document and have been deemed receivable. This pragmatic approach acknowledges records which are in reality "unavailable and

---

[91] While the data can be said to be "filed" electronically in these media, the files themselves are in reality magnetic files.

useless except by means of the printout sheets" as was discussed in *King v State ex rel Murdock Acceptance Corp.*[92]

2.139 In the case of so called "optical disk files" (for example, CD-ROM), the information is strictly speaking etched onto the surface of a specially coated disk with a laser beam. Although the information stored on an optical disk is in effect a "bit-pattern 'image' of optically scanned literal, graphic or pictorial information (as opposed to binary-coded characters),"[93] it is nonetheless machine-readable and, in the absence of statutory or case law to the contrary, should be treated as analogous to that information stored on magnetic disk or tape when determining its admissibility and veracity.

2.140 Allowance was made in the ever-expanding milieu of electronic record storage and maintenance in Rule 1001 (1) of the US Federal Rules of Evidence, providing that writings and recordings consist of any of the penumbra of "letters, words, or numbers, or their equivalent, set down by... magnetic impulse, mechanical or electronic recording, or other form of data compilation."

2.141 This lies alongside the seemingly rigid Rule 1002 of the Federal Rules of Evidence which states that "(t)o prove the content of a writing, recording or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." The Federal Rules of Evidence then go on to provide otherwise and make allowance for duplicates, public documents etc.[94]

2.142 A duplicate is deemed admissible to the same extent as an original save where a genuine question is raised as to the authenticity of the original or where in the circumstances it would be unfair to admit the duplicate in place of the original.[95]

2.143 As in other statutory regimes across the world, exceptions are made for admitting the contents of an official record, or of a document authorised to

---

92 222 So.2d 393, 398 (Miss. 1969).

93 Taken from A Guideline for Federal Records Managers or Custodian, from the Electric Law Library's "Admissibility of Electronically Filed Federal Records as Evidence" paper available at www.lectlaw.com/files/crf03.html, p 3.

94 With regard to duplicates and public or official records, the rules state in pertinent part as follows:

A "duplicate" is a counterpart produced by the same impression as the original,.. or by mechanical or electronic re-recording,... or by other equivalent techniques which accurately reproduce the original. Federal Rule of Evidence 1001(4).

95 Federal Rule of Evidence 1003.

be admitted by means of the provision of a certified copy (where certified by a witness who has compared it with the original). If such a copy cannot be obtained by the exercise of reasonable diligence, then other secondary evidence of the contents may also be given in disregard of the strictures of the Best Evidence Rule.[96]

2.144 In the US at Federal level, Rule 1001(3) of the Federal Rules of Evidence makes specific allowance for what does and what does not constitute an "original" for the purposes of satisfying the Best Evidence Rule in the US. Under this provision an original of a writing or recording is deemed to be the writing or recording itself or "any counterpart intended to have the same effect by a person executing or issuing it.... If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately" is also deemed receivable as an original.

2.145 These centralised rules then seem to contemplate many species of document including duplicates, or copies of official records, additional printouts of the same information contained in a magnetic file produced at different times, as well as carbon or photocopied copies as originals for the purposes of admitting electronic and automated documentary evidence.

(b) The Californian Approach

2.146 The Californian Law Revision Commission recommended that the rules permitting secondary evidence should not include oral testimony of the contents of a written statement because of the inability to decisively establish standards and safeguards where individuals cannot be expected to retain total recall of the exact contents of a written memo.[97] This can be viewed as a means by which to overcome situations analogous to the *Myers* scenario. Having incorporated this into their revised code, section 1523 of the Code now provides that oral testimony of contents can only be admissible in certain limited circumstances including instances where the original has been lost or destroyed.

2.147 To this end, section 1523 of the Californian Evidence Code provides:

> (a) Except as otherwise provided by statute, oral testimony is not admissible to prove the content of a writing.
> (b) Oral testimony of the content of a writing is not made inadmissible by subdivision (a) if the proponent does not have possession or control of a copy of the writing and the original is lost or has been

---

96 Federal Rule of Evidence 1005.

97 Californian Law Revision Commission Recommendation on the Best Evidence Rule *Best Evidence Rule,* 26 Cal L Revision Commission Reports 369 (1996).

destroyed without fraudulent intent on the part of the proponent of the evidence.

(c) Oral testimony of the content of a writing is not made inadmissible by subdivision (a) if the proponent does not have possession or control of the original or a copy of the writing and either of the following conditions is satisfied: (1) Neither the writing nor a copy of the writing was reasonably procurable by the proponent by use of the court's process or by other available means. (2) The writing is not closely related to the controlling issues and it would be inexpedient to require its production.) Such a guarded stance, cautious in its approach yet universal in its application to oral testimony when submitted as secondary evidence to substantiate documentary evidence is appropriate given the potential difficulties in a witness' ability to accurately pronounce on the contents of a document from memory.

2.148 The Californian Evidence Code provided in s 1500 (as amended) that other than provided by statute, no evidence except the original of a writing was to be admissible to prove the content of a writing. This section (cited as the Best Evidence Rule) applied only to the proof of the contents of a "writing," defined broadly to includes:

> "handwriting, typewriting, printing, photostating, photographing, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof."

2.149 Therefore it can be said that in the US, the Federal Rules of Evidence rule 1001(3) stating that "if data are stored in a computer…, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" This scuppers any application of the best evidence rule.

2.150 US courts rarely bar printouts under the best evidence rule. In *Aguimatang v California State Lottery*,[98] the court gave near *per se* treatment to the admissibility of digital evidence stating "the computer printout does not violate the best evidence rule, because a computer printout is considered an 'original.'"

(5) Reform

2.151 In the Commission's view, the replacement of the Best Evidence Rule would mean a simpler doctrine making secondary evidence other than oral testimony generally admissible to permit the document to speak as to its own proof in the case of documentary evidence. This would provide sufficient

[98] 234 Cal App 3d 769 at 798.

protection in civil cases and, with slight modification, in criminal cases where the changes made in section 30 of the *Criminal Evidence Act 1992* have already broadly replaced the Best Evidence Rule. Given the rigidity of the Best Evidence Rule it has, by necessity, attracted broad exceptions and the Commission has therefore concluded that removing this inflexible rule would not be a dramatic change in existing practice. It would instead make the law more straightforward and efficient. The Commission is of the opinion that the proposed statutory framework in the form of an *Evidence Bill* should, therefore, replace the Best Evidence Rule in its entirety and suggests the abolition of the Best Evidence Rule, namely the rule of evidence to the effect that an original piece of evidence, particularly a document, is superior to a copy and that if the original is available, a copy will not be allowed as evidence in civil or criminal proceedings. In its place, the proposed statutory framework on documentary evidence should contain a rule that documentary evidence is, in general, admissible in proceedings where the court is satisfied as to its relevance and necessity.

2.152 The Commission provisionally recommends the abolition of the Best Evidence Rule, namely the rule of evidence to the effect that an original piece of evidence, particularly a document, is superior to a copy and that if the original is available, a copy will not be allowed as evidence in civil or criminal proceedings.

2.153 The Commission also provisionally recommends that, in its place, the proposed statutory framework on documentary evidence should contain a rule that documentary evidence is, in general, admissible in civil and criminal proceedings where the court is satisfied as to its relevance and necessity.

2.154 An inclusionary approach through the replacement of the Best Evidence Rule would see documentary evidence admitted where the court is satisfied as to its relevance. This would give statutory effect to the principle that there are no degrees of secondary evidence and any issues as to authenticity, integrity and reliability would go to weight. The Commission examines the weight to be attached to such evidence in Chapter 5, and for present purposes turns to set out the provisional conclusions it has reached on this aspect of the law.

E The Second Exclusionary Rule of Evidence- the Rule Against Hearsay

2.155 Where a document is submitted as evidence of the truth of its contents, the document is admitted for a "testimonial purpose" which means that the party is effectively offering written testimony in place of a witness giving oral testimony in court. Unless the document can be brought within one of the common law and statutory exceptions to the rule this attempt to introduce a document as proof of any statement contained therein, otherwise than by

providing oral testimony of a witness who appears in court, would infringe the rule against hearsay.

(1) The Best Evidence Rule and its Interaction with the Hearsay Rule

2.156 Both the Rule against Hearsay and the Best Evidence Rule focus on reliability as the primary object by which to judge admissibility. The Best Evidence Rule attempts to ensure reliability by requiring that the source document be secured and produced to the court and that this source document created prior to, rather than in anticipation of litigation is likely to be accurate and honestly recorded. As this is not always possible and where a sufficient explanation is offered, the Best Evidence Rule may be satisfied by the production of a copy which is demonstrated to be a true copy. This will normally be by way of oral evidence from someone in a position to compare the original with the copy.

2.157 Where documentary evidence is produced as proof of itself simply to establish that the information was sent, received or stored, the document in question counts as real, direct evidence which is not automatically excluded as is its counterpart - a document produced as proof of its contents which may infringe the rule against hearsay. The law excludes a document as hearsay owing to questions as to the reliability of the content rather than doubt as to the reliability of the technology used to record that content.

(a) Extent of the Hearsay Rule

2.158 A document is hearsay because it is a second-hand representation of information about a matter to which the statements in the document relate, as opposed to statements made by an eye-witness who can be cross-examined. Such evidence is in the main inadmissible unless it falls into a statutory or common law exception.

2.159 Given that one of the fundamental principles of the common law is that the best evidence; the original, must be offered in evidence in order to satisfy the requirements of evidential rules, interaction with the rule against hearsay is unavoidable.

(b) The Development of the Hearsay Rule and the Best Evidence Rule – the Position Under English Law

2.160 Although there had been some limited reforms in English law addressing particular forms of proof of documents and statutory certificates of declarations of certain facts, such as registers of births, deaths and marriages and entries in bankers' books the first major reform was the *Evidence Act 1935*. It reformed the Hearsay Rule in civil proceedings by providing new

exceptions for specific categories of documents but applied only to the literal concept of documentation. Oral hearsay was left to the common law rules.

2.161 This was followed by the *Civil Evidence Act 1968*. Section 2 of the 1968 Act, which governed the admissibility of hearsay evidence in most civil proceedings, made all first-hand hearsay and a great deal of second-hand hearsay admissible provided certain conditions were satisfied.[99]

(2) Exceptions to the Strict Application of the Exclusionary Rules in Other Jurisdictions

2.162 Exceptions tolerated in other jurisdictions which forgo the necessity of having to produce the primary or original document include circumstances where the document has been lost or destroyed or where it is known to be in the possession of another who has refused to discover the document or has acted so as to be negligent in the production of that document following due notice requiring production. Another exception dispensing with the Primary Evidence Rule occurs where the party in possession claims a privilege to so withhold and which he refuses to waive.

2.163 Therefore where it is physically impossible or even where merely highly inconvenient to produce the documentary evidence because of the material's physical characteristics secondary evidence will be receivable by the court. Examples include where the document in question was purported to be characters engraved on a tombstone (the *Tracy Peerage Case)*[100], or chalked onto the side of a building approved (*Sayer v Glossop*[101] and *Mortimer v*

---

99 Section 1(1) provided:-

"In any civil proceedings a statement other than one made by a person while giving oral evidence shall be admissible as evidence of any fact stated therein to the extent that it is also admissible by virtue of any provision of this part of this Act or by virtue of any other statutory provision or by agreement of the parties, but not otherwise."

Section 2(1) stated:-

"In any civil proceedings a statement made, whether orally or in a document or otherwise, by any person, whether called as a witness in those proceedings or not, shall, subject to this section and to the rules of court, be admissible as evidence of any fact stated therein of which direct oral evidence by him would be admissible."

100 10 Cl & F.

101 2 Exch 411.

M'Callan[102]) or even where the information required is contained in a banner permanently affixed to a wall.[103] In *Sayer v Glossop* Pollock CB also recognised the need to be able to produce something to the court in place of the primary evidence where the primary documents in question are otherwise unattainable. Representative evidence would then be acceptable before the court where for example, if, "in point of law you cannot compel a party who has the custody of a document to produce it, there is the same reason for admitting other evidence of its contents as if its production were physically impossible."[104]

2.164 These exceptions permit the court to receive secondary or derivative evidence as a representation of the impugned evidence. They are received as legitimate evidence and are inferior to primary evidence solely in respect of their derivative character which the courts are willing, and legislatively permitted to overlook.

(a) Australian Hearsay Provisions

2.165 Section 59 of the Uniform *Evidence Act 1995* reaffirms the hearsay rule but its stringency is tempered by later sections which allow a number of exceptions. For the purposes of electronic documentary evidence these include section 71, which applies to electronic mail, fax, telegram, lettergram and telex and which provides that the hearsay rule does not apply to statements in such messages as to:

(a) the identity of the originator;

(b) the date and time of dispatch;

(c) the destination or identity of addressee.

2.166 This section incorporates many of the hearsay issues in that area of electronic commerce which is concerned with contract formation as most categories of data messages will have no hearsay component outside the issues in (a), (b) and (c). Section 71 makes it unnecessary to call as a witness those persons most likely to be able to throw light upon these issues.

2.167 A further exception in section 63 (2) is where the maker of the impugned hearsay statement is "unavailable" meaning dead, not competent, or where it would be unlawful for that person to give evidence or if reasonable steps have been taken to secure or indeed compel attendance but which have been unsuccessful. While notice of intention to introduce such evidence must be given and though failure to so notify ought to waive the statutory exception

---

102 6 M & W 63 and 68.

103 R v *Fursey*, 6 C & P 84 and *Jones v Tarleton* 9 M & W 675.

104 (1848) 2 Exch 409, 441.

the court retains a general residual power to dispense with the notice requirement.

2.168 Further to the specific issues of identity of originator, time and date of dispatch, the Hearsay Rule may be important in other areas to do with contract. Computers are widely utilised for archiving purposes where original letters are generated or stored. Also, Nicoll[105] identifies that "banking, inventory and accounting records may be stored by computer after having been keyed in by a human operator" and that these too may be wholly or partially hearsay.[106]

2.169 In most instances the recording of this type of data will be regular and repetitive. Section 69 makes specific allowance for business records and creates an exception for hearsay assertions in documents made by a party who had or might reasonably be supposed to have had personal knowledge of the asserted fact. If a party seeks to introduce hearsay evidence to prove that a particular record was not kept, section 69(4) creates an exception where:

> (a) the occurrence of an event of a particular kind is in question; and
>
> (b) in the course of a business, a system has been followed of making and keeping a record of all events of that kind.

(b) Public documents in Australia

2.170 Part 5, Division 1 of the *Evidence Act 1997 (Qld)* contains a number of provisions that deem certain public documents to be evidence as to the truth of their contents when proved in court in a specified manner.

2.171 The prevailing rationale in providing the proof of such documents is to relieve the parties of the burden of mounting expenses or the practical as opposed to legal inconvenience in trying to establish their authenticity. The provisions re-enact the common law exception to the secondary evidence rule afforded to public documents.

2.172 Statutory provisions in all Australian territories allow for certified copies of public documents to be admitted as though they were originals.

(c) Paper v Electronic Form

2.173 The provisions in Part 5, Division 1 of the *Evidence Act 1977* (Qld) display a preference and deference for physical paper documents and the vocabulary used seems to foresee the use of these hard documents rather than

---

105 Nicoll, *Should Computers be Trusted? Hearsay and Authentication with Special Reference to Electronic Commerce*, Journal of Business Law, 1999, Jul, 332-360.

106 For a discussion on electronic evidence as real or hearsay evidence see below paragraph 5.41-5.48.

documents in electronic form, particularly in relation to the certification of public documents. This is evident from section 51 of the *Evidence Act 1977* (Qld) which provides:

> "Where a document is of such a public nature as to be admissible in evidence on its mere production from proper custody, a copy of or extract from the document shall be admissible in evidence if—
>
> (a) it is proved to be an examined copy or extract; or
>
> (b) it purports to be certified as a true copy or extract under the hand of a person described in the certificate as the person to whose custody the original is entrusted."

2.174 The *Evidence Act 1995* (Cth) does not seem to have dramatically reformed this approach and has in reality adhered to and restated this position. For example, section 156 of that Act provides:

> "(1) A document that purports to be a copy of, or an extract from or summary of, a public document and to have been:
>
> (a) sealed with the seal of a person who, or a body that, might reasonably be supposed to have the custody of the public document; or
>
> (b) certified as such a copy, extract or summary by a person who might reasonably be supposed to have custody of the public document;
>
> is presumed, unless the contrary is proved, to be a copy of the public document, or an extract from or summary of the public document.
>
> (2) If an officer entrusted with the custody of a public document is required by a court to produce the public document, it is sufficient compliance with the requirement for the officer to produce a copy of, or extract from, the public document if it purports to be signed and certified by the officer as a true copy or extract.
>
> (4) The court before which a copy or extract is produced under subsection (2) may direct the officer to produce the original public document."

2.175 The underlying principle for this legislative restatement arises where a court is presented with a document which the propounding party seeks to adduce as evidence of the truth of the contents. Despite this being for example for a public document, evidence is still required to establish the authenticity of a copy as the public nature of this public document might be considered so serious that the authenticity of a copy of, or extract from, the public document should be beyond doubt. A manual certification by an appropriate officer on the

authenticity of a copy of, or extract from, the public record might not be considered an excessive requirement in the circumstances.

(3) Proof of the Truth of Statements Contained in "Documents" for the Purposes of the Exclusionary Rules

2.176 The Best Evidence Rule also interlocks with the operation of the Hearsay Rule namely that a party should adduce the best evidence possible in making his claim and requires the party to show the documentary evidence is the original version although it will be considered in isolation from it. The Rule typically applies when the contents of the writing are at issue and also when a witness testifies as to a fact of having read it in the document which is presented in evidence. The common law rule against hearsay excludes evidence where it represents an assertion other than one made by a person while giving oral evidence in the proceedings and makes it inadmissible as evidence of any fact or opinion so asserted.

(4) Transcript Documentary Evidence in Criminal Proceedings

2.177 Where transcripts are adduced in criminal proceedings 4(f) of the *Criminal Procedure Act 1967* as amended by section 9 of the *Criminal Justice Act 1990* provides that evidence may be given at trial where these take the form of a transcript.

(5) Transcript Documentary Evidence in Civil and Non-Adversarial Proceedings

2.178 In *Borges v Fitness to Practice Committee of the Medical Council*[107] the applicant sought an injunction restraining the admission of documentary materials which were obtained from proceedings undertaken before the General Medical Council of the UK. The impugned documentary materials were transcripts of the findings of the Medical Council, the report on these proceedings and the transcripts of the judgment of the Privy Council which the respondent sought to have admitted into evidence in the course of a disciplinary hearing in Ireland. When the matter came before the Supreme Court the applicant contended that these documentary materials ought not to be admitted on several fronts. These included the hearsay element of the transcripts where the respondents did not propose to offer oral witness testimony on the matters concerned: the applicant claimed the transcripts were being offered as documentary hearsay and as evidence of the proof of the matters contained therein in order to support a finding of professional misconduct. Other arguments were based on the applicant's rights to fair procedures and protection of his constitutional rights under Article 40.1.

---

107 [2004] 1 IR 103.

2.179 The question was whether section 45 (3)(b) of the *Medical Practitioners Act 1978* envisaged documentary as well as oral evidence being admitted before the Fitness to Practice Committee and permitted documentary hearsay where this was admissible as evidence. *Goodman v Hamilton*[108] made it clear that tribunals of inquiry are not bound to adhere to the strict rules of evidence. Instead the focus is on fair procedures and as such where "a question arises as to the receipt of hearsay evidence the Tribunal might be required to hear person affected on the point".[109]

2.180 While tribunals of inquiry exercise their functions more casually and often depart from evidential norms and receive previously unsworn essentially hearsay evidence "they may not act in such a way as to imperil a fair hearing or a fair result" as the Supreme Court held in *Kiely v Minister for Social Welfare.*[110]

2.181 Opposing counsel focused on the inability of the Medical Council's Committee to compel witnesses to attend and that even where available, their cross-examination would be an artificial means of tendering evidence already available. The High Court was of the opinion that the hearing should not proceed on the basis of the transcripts in the complete absence of "oral testimony of the central witnesses, the complainants, against the applicant" and would amount to a deprivation of justice.

2.182 The Supreme Court affirmed the High Court's judgment and in doing so appeared to put the hearsay matters arising in *Myers* firmly to rest.

2.183 Along with disciplinary hearing another example of documentary Evidence in non-adversarial proceedings is the discrete area of proceedings at a coroner's inquest. The coroner is entitled to admit non-contentious documentary evidence where the parties affected by the admission of the evidence have been notified and the coroner has made his intention to admit the evidence known. Following the Report of the Working Group on the Review of the Coroner Service where objection is made to documentary evidence being admitted and making up the main of the evidence, the coroner is under an obligation to adjourn the inquest.[111]

2.184 The rules of evidence as applicable in a legal setting do not apply in the Coroner's Court which is an inquisitorial rather than an adversarial court. In

---

108 [1992] 2 IR 542.

109 *Ibid,* at 565.

110 [1977] IR 276 at 281.

111 Report of the Working Group on the Review of the Coroner Service 2000, Part 6.7.

consideration of the application of the rules of evidence to coroners' inquests Lord Lane CJ stated in *R v South London Coroner ex parte Thompson*[112] that:

> "the procedure and rules of evidence which are suitable for one [the adversarial court processes of the courts] are not suitable for the other. In an inquest it should not be forgotten that there are no parties, there is no indictment...It is an inquisitorial process, a process of investigation quite unlike a trial."

2.185 Documentary evidence including documentary hearsay evidence is admissible at an inquest and while the coroner may be susceptible to a judicial review of the exercise of his power, there is no appeal from the verdict of an inquest.

(6) Legislative Admissibility of Hearsay Documentary Statements in Civil Proceedings in Australia

2.186 Section 92 of the *Evidence Act 1977* (Qld) is derived from the *Evidence Act 1938* which made admissible as documentary evidence in civil cases certain kinds of hearsay statements that tend to establish a fact. This development resulted from a need to legislatively overcome the difficulties that emerged in trials in relation to the admission of commercial documents.

2.187 In 1939 Lord Maugham LC offered this explanation for the English *Evidence Act 1938* commenting on the then newly-implemented statute's utility.

> "During my long time at the Bar I came across a number of cases in which had it been in force, would have been of extraordinary value. I have had cases in which it was necessary to prove reports by engineers as to the value of ore deposits…in distant lands …circumstances connected with landing facilities…on a distant island…[But] before the recent Act, such a report…could never be put in evidence. The engineer in many cases could be called, but even then he could use his report to refresh his memory, but not for any other purpose."[113]

2.188 Part VI of the *Evidence Act 1977* (Qld) advances the view which is incorporated in sections 92 and 93. The provision which enables documents which would otherwise be excluded as remote documentary hearsay to be admitted applies only where direct oral evidence of a fact would be admissible and where documents contain statements that would tend to establish such a fact (section 92(1)). At common law, a statement in a document asserting a fact as something within the personal knowledge of the statement-maker would

---

112 (1982) 126 SJ (625).

113 (1939) 17 Can Bar Rev at 481.

generally be inadmissible. This is because, if the statement is offered as a true narrative of the events in issue, the statement is made out of court and is not subject to cross-examination.

(i) Requirements for admissibility under section 92

2.189 The main requirement for admissibility under section 92 and similar provisions in other jurisdictions is that the maker of the statement must have personal knowledge of the matters dealt with in it, or in the alternate that the record is a record of an undertaking (or a business record) that contains statements made from information supplied by those with personal knowledge of the matters recorded. Statements in records will then be admissible even where the information has passed through several hands. A second requirement is that the maker of the statement must be called as a witness unless he or she is unavailable for one of the reasons specified in section 92(2).

2.190 Section 92 enables two types of documentary hearsay evidence to be admitted in civil cases: statements that record the personal experience of the statement-maker and those documented in the ordinary course of an "undertaking".

2.191 In proceedings where the maker of a statement had personal knowledge of the matters dealt with in the statement and is called as a witness, the statement will be admissible as evidence of the matters in it.[114] If the maker of the statement is not available to give evidence for certain specified reasons (such as that he or she has died or is out of the State), the statement will still be admissible as evidence of the matters recorded therein.[115]

2.192 The operation of section 92 is subject to a number of provisions in Part 6 of the *Evidence Act 1977* (Qld) which provides for the exclusion of evidence where eg it appears as per section 98 to the court that it would be "inexpedient in the interests of justice that the statement should be admitted" or where the jury might afford the document a degree of prejudicial weight to which it is not entitled.[116]

(b) Admissibility of Statements in Documents in Criminal Proceedings

2.193 Section 93 of the *Evidence Act 1977* (Qld) is similar to section 92, but applies to criminal proceedings. This division of evidential labour is possibly due to the higher standard of proof in criminal matters and therefore higher degree

---

114 Section 92 (1)(a).

115 Section 92 (1)(a) and (b).

116 Section 99.

of difficulty to admit a statement in a document as evidence of the matters in the statement in criminal proceedings than in civil proceedings.

2.194 Section 93 of the *Evidence Act 1977* (Qld) is based on the English *Criminal Evidence Act 1965* which was itself a response to the difficulty encountered in *Myers v Director of Public Prosecutions*.[117]

2.195 The Commission notes that were such records sought to be admitted today, they would most likely be admissible as records of a trade or business.

(7) Concluding Observations on Hearsay

2.196 A point of divergence between the various ways in which different jurisdictions approach matters of hearsay relates not so much to its definition or exceptions but instead focuses on the procedural safeguards provided for the testing and filtering process for evidence before the commencement of proceedings. In this process there remains an uneasy tension between the requirement that to be admissible, the evidence ought to be reliable and the practical difficulties of dealing with large amounts of evidence which may be scattered across numerous mediums and jurisdictions.

F Conclusions on the Problem of Electronic and Automated Documentary Evidence and the Exclusionary Rules of Evidence

(1) Shifting the Focus of the Law of Evidence

2.197 The proliferation of electronic media has created a number of new and peculiarly unique problems for the law as many evidential rules assume the existence of paper records, of signed records or of original records as a default position. The law of evidence was traditionally also relied on paper records, though oral testimony and physical objects have always been part of the courtroom proceedings. As more and more legal, commercial and leisure activities are carried out by electronic instruments the need to regulate this source of evidence, to lay down conditions of admissibility and to demonstrate the legal rights that flow from them has gained momentum. This is because many records managers and their legal advisors have not been confident that modern information systems, especially electronic imaging where the paper originals have been destroyed, will produce suitable records for use in court.

2.198 However, the regulation associated with this type of evidence cannot be taken as symptomatic of an evidential crisis and indeed the law as it currently stands, while cumbersome, time-consuming and unwieldy is not badly broken. Most electronic documentary records are being admitted in practice.

---

117 [1965] AC 1001, discussed at paragraph 2.109 above and paragraph 5.33 below.

But courts have struggled with the traditional rules of evidence and adapting these to newer technologies with predictably inconsistent results. Common terms such as "reliability" have caused confusion between the principles of authentication, best evidence (just how suitable is the continued application of this largely redundant rule to electronically generated documents?), hearsay and weight. The Commission is of the opinion that the law requires some streamlining to ensure greater efficiency and predictability to ensure against incompatibility with modern means of producing and maintaining documentary evidence.

(2) The Best Evidence Rule

2.199 The Commission is of the opinion that the Best Evidence Rule as the primary evidential weapon excluding documentary evidence from proceedings in no longer viable as concerns the modern means of conducting evidence inquiries.

2.200 Among the few positive modern judicial supports for the Best Evidence Rule is the English case *R v Wayte*[118] in which Beldam J noted a possible use for the Rule. He stated "it is now well established that any application of the best evidence rule is confined to cases in which it can be shown that the party has the original and could produce it but does not."[119] The court seemed to imply that if this were the case the court would be entitled to infer the worst about the provenance of the document and would exclude the copy. The judge was of the opinion that the result of following such a course meant that the law of evidence through the courts was "cutting down still further what remains of the Best Evidence Rule, [and with which result] we are content."[120]

2.201 The Best Evidence Rule requires the proponent of evidence to produce the best evidence available to that party and which the circumstances of the case are amenable to. In practice this has generally required the production of the instrument closest to the original document. The Best Evidence Rule begs the question of just how close is the current document to its "original" version? Has its integrity been maintained consistently or are there differences between the record and its "original" version?

2.202 This presents two challenges peculiar to electronically-generated documentary evidence.

---

118 (1982) 76 Cr App R 110.

119 *Ibid,* at 116.

120 *Ibid.*

2.203 Broadly speaking electronic data records do not have a meaningful "original", and nor are they amenable to identifying an original that is distinguishable from their display on a screen or by printout. No one production or reproduction is categorically closer to the electronic document than another, any more than one printout is more original than any other from the same electronic data.

2.204 Another point centers on those who transfer paper records to electronic images and want to destroy the paper originals, motivated by saving storage costs and the idea of easier document management. Were insistence focused on the Best Evidence Rule in relation to computer records this deliberate although not necessarily fraudulent or destructive practice would be halted. Otherwise the possibility would remain for tribunals to judge such deliberate destruction of originals harshly when viewed under a literal reading of the Best Evidence Rule as the originals themselves would not be available as a result of the deliberate act of the party seeking to rely on the record.

2.205 Solutions which have evolved in consequence to problems associated with paper-based records cannot be fully adept at addressing the quandaries thrown up by distinctly electronic records. Courts and legislatures have attempted to characterise printouts as originals, or as duplicates of an original core data base, or in the default, as reliable copies. Some reform proposals have also tried to create a category of "duplicates" which would include photocopies, certified true copies, and electronic images, and which would be considered equivalent to the original for the purpose of satisfying the Best Evidence Rule. These attempts are all artificial constructs provoked as a reactionary response to the Best Evidence Rule.

2.206 If the Best Evidence Rule were retained in the law of evidence I (even taking account of the inclusionary exceptions), the law would run the risk of incompatibility with modern techniques of communication and information systems. This would frustrate the proper determination of disputes and see relevant documents excluded for the sake of compliance with a common law rule whose utility has long since passed.

2.207 In the case of electronic and automated documentary evidence, some jurisdictions have legislated on electronic evidence, but not consistently with each other. As a result, businesses which are active in more than one jurisdiction may have to keep records differently for use in different disputes.

2.208 Furthermore, any proposed abolition of the Best Evidence Rule as it applies in relation to electronic records would not affect the question of the weight that the court might accord to a particular piece of evidence as alluded to by Dawson J in *Butera's* case:

> "Of course, some modes of proof are better than others, but that, save in the case of written documents, goes to weight rather than admissibility."

2.209 With the dissolution of the Best Evidence Rule some examination of the term "original" and whether maintaining this term in its colloquial form is convenient would be resolved. The idea would be to shift the meaning of the word "original" in the context of documentary evidence. Rather than fall foul of the rule against hearsay, a re-defining of the concept would mean that, where available, a primary source document would still be adduced to the court. However the Commission envisages that the new labeling of an original would neutralise the concept of an original and remove the strictures of the Best Evidence Rule which could then be removed.

2.210 With this in mind the Commission considers that the law on evidence should be reformed so that public and private sectors alike can make the best technical decisions possible about how to produce and keep records, with a minimum of uncertainty about how their legal rights will be affected.

2.211 The Commission considers that the removal of the Best Evidence Rule with its many exceptions as a means of regulating the admissibility of derivative electronically-generated evidence in both civil and criminal proceedings would resolve many of the difficulties in the area of documentary evidence. The removal of the Best Evidence Rule requiring the search for original records or another format as good as an original would alleviate many of the problems associated with electronic records and accommodate continuing technological innovation.

2.212 This would leave the way clear for admissibility to be based on the sole criterion of determining the relevance of the document coupled with the exercise of judicial discretion prior to any evidence being admitted, whether in civil or criminal cases. It would also accommodate the use of both paper and electronic and automated documents produced through technology by adopting a technology-neutral approach to evidence rather than establishing a parallel e-evidential system to isolate and resolve technology based evidential issues. This is not to imply that technology can be applied without regard to form. It means that the way the law will apply to technological choices should be as certain as possible, so those choices can be made for clearly articulated reasons. The Commission thus concludes that the rules of evidence which address the need to produce an original of an electronic or automated document be interpreted to mean presenting a reproduction in legible form including in printed form a copy or derivative of an electronic document.

2.213 The Commission provisionally recommends that the rules of evidence concerning the need to produce an original of an electronic or automated document be interpreted to mean presenting a reproduction in

legible form (including a printout) or a copy or derivative of an electronic document.

2.214 This would mean a legislative equality as between the production of an original in terms of an electronic document and the production of a copy or derivative in legible form in line with disparate legislation in the area[121] would remove any linguistic preference to hard paper documentation over its electronic counter-part be removed and that digital evidence be brought on a par with its traditional paper counterpart.

[121] Eg section 131 of the *Central Bank Act 1989*.

CHAPTER 3 PUBLIC RECORDS AND DOCUMENTS AS EVIDENCE

3.01 In Part A of this Chapter the Commission discusses public documents as a prominent exception to the exclusionary rules of evidence. It investigates how to establish and introduce the proof of the contents of these documents by establishing that the document records information relating to a public matter, that the person compiling the information has a public duty to so record, that the document is set to have some longevity about it and is to be retained and that it would be available for public inspection.

3.02 Part B goes on to examine the various forms of public documents as verifiable documentary evidence - public records admissible under existing legislation, documentary evidence of certain professional qualifications, judicially noticed official documents (both domestic and international). It examines the characteristics which determine whether a record is a public document so as to avoid the strict application of the exclusionary rules of evidence.

3.03 Part C examines private documents from a similar perspective with focus on the means by which to establish the proof of the record in question; its authorship or chain of custody by means of comparison, by adducing proof of handwriting or opinion evidence. The Commission also recommends that the current distinction ought to be retained as between public and private documents for the purposes of admissibility as evidence.

A Public Documents Admissible as an Exception to the Exclusionary Rules of Evidence

3.04 The exception to primary documentary evidence was extended at common law to permit secondary evidence of the contents of public documents given the practical and monetary inconvenience inherent in the production of the originals.[1]

3.05 Public documents will usually be taken as *prima facie* admissible as evidence and do not require further authenticating testimony. The standard will

[1] See *Mortimer v M'Callan* (1840) 6 M & W 58 at 68.

be met by simply showing that they are printed by official government printers and bear the stamp, seal or signature of certain officers or departments or by a private entity which has had the task delegated to it and therefore prints under the auspices of the Stationary Office or a public procurement office.

(1) Determining Whether a Document is a Public Document to Fall within the Exception

3.06 Public documents are therefore admissible as evidence of the truth of their contents. This was demonstrated in *Wilton & Co v Phillips,*[2] the rationale of which was approved in *Irish Society v Bishop of Derry*[3] by Parke B and later extended to foreign governments' records in *Lyell v Kennedy*.[4]

3.07 *Irish Society v Bishop of Derry* by Parke Bstated:

> "In public documents, made for the information of the Crown...the entry by a public officer is presumed to be true when it is made, and it is for that reason receivable in all cases, whether the officer or his successor may be concerned in such cases or not."

3.08 This analogy was extended to public census documents in *Dublin Corporation v Bray Township Commissioners*[5] where it was stated that the census "is a public paper made out by public officers under a sanction and responsibility which impel them to make it out accurately".

3.09 To this end, public documents are considered to be sufficiently reliable to permit their admission without recourse to other formalities. This is so as to avoid any frustration to the administration of justice in circumstances where public documents are concerned given that their longevity is the rationale for their being excused the operation of the stricture of the exclusionary rules of evidence. This could occur following the death of the public official who was responsible for creating the document in question. A secondary motive is the likely inconvenience which would arise were public servants required to attend to give testimony as to the content of a document as well as the probability that much of the knowledge which gave rise to the document has been forgotten given the mundane nature of many administrative recordings.

3.10 Not all public documents will, however, be admissible. The English case *Sturla v Freccia* is an example of this. This case related to a report compiled by a committee at the behest of the Genoese government as to the

---

2 (103) 19 TLR 390.

3 (1846) 12 Cl & Fin 641.

4 (1889) App Cas 437 at 448-9 (Lord Selbourne).

5 [1900] 2 IR 88 at 93.

suitability of a candidate for a government post. This report which contained details of the candidates age was held not to be sufficient evidence of its contents as it was not a public matter and nor was it for public inspection. It was not intended to be retained and it was not the purpose of the committee to investigate the matters which the report contained. Lord Blackburn[6], said he understood

> "a public document to mean a document that is made for the purpose of the public making use of it, and being able to refer to it. It is meant to be where there is a judicial or quasi-judicial duty to inquire..."

3.11 Essentially, there must be present four basic precursors to determine whether a document is an admissible public record:[7]

i) A public duty to inquire and record - the person compiling it must be under a public duty to satisfy himself or herself of the truth of the statement.[8]

ii) A public matter.[9]

iii) Retention - the document must have been created for the purpose of being retained and not on a temporary basis.[10]

iv) Public inspection - the document should be available for inspection by the public.[11]

---

6 [1926] Ch 284 at 318.

7 See also *Cross and Tapper on Evidence* 11th ed, (Oxford University Press, 2007) p 633.

8 *Doe d France v Andrews* (1850) 15 QB 756 (Erle J).

9 *R v Halpin* [1975] QB 907. This case concerned a charge of conspiring to cheat and defraud. A file from the Companies Register was sought to be admitted as it detailed the annual returns filed under the Companies Act. The court held that the requirement that the document be concerned with a public matter need not necessarily mean it must be of concern to the whole of the public and that the annual returns were admissible.

10 *Heyne v Fischel & Co* (1913) 30 TLR 190; *Mercer v Dunne* [1905] 2 Ch 538; *White v Taylor* [1969] 1 Ch 150.

11 An example of this is visible in a case concerning the *Perjury Act 1911 -Lilley v Pettit* [1946] KB 401). The question here was whether a false declaration had been made as to the paternity of a child. The prosecution was unsuccessful in its proposal to have certain documentary evidence admitted as an exception to the hearsay rule. It was alleged that the man in question could not be the child's

3.12 Section 188 of the English *Criminal Justice Act 2003* placed the common law exceptions to the exclusionary rules on a legislative footing for the purposes of the criminal law. Reform of the equivalent rules in civil litigation had been made many years before and is now codified in the English *Civil Evidence Act 1995.* This provision represents a considered approach which preserves some of the stated exceptions while abolishing the remaining common law categories of admissibility. The categories maintained are broad and inclusive and include "public information etc."[12] legislating for the admissibility of published works,[13] public documents,[14] and state records,[15] and the details pertaining to registration of births, deaths and marriages.[16]

3.13 In respect of other less formal species of public documentation it must also be noted that there is no requirement that the documents here referred to be generated contemporaneously with the events which it records. In the English case *R v Halpin* it was held that this is a matter which goes to weight rather than admissibility.[17]

3.14 To determine whether a document is a public document and deserving of such special treatment the following basic canons must be established. The matter must be of a public nature. Lord Blackburn, in *Sturla v Freccia*[18], said:

> "a public document to mean a document that is made for the purpose of the public making use of it, and being able to refer to it. It is meant to be where there is a judicial or quasi-judicial duty to inquire..."

---

father as he had been billeted overseas at the date of the child's conception. The court held that statements in public documents (here the prosecution sought to introduce military records from the War Office) could be admitted as prima facie evidence of the facts contained therein. These would qualify as an exception to the hearsay rule where the documents were shown to be accessible to the public and kept for the information of the public. This could not be demonstrated here as the records were solely for governmental administrative use and so were deemed inadmissible.

12 Section 118 (1)(1).

13 Section 118 (1)(1)(a).

14 Section 118 (1)(1)(b).

15 Section 118 (1)(1)(c).

16 Section 118 (1)(1)(d).

17 [1975] QB 907 at 913.

18 [1926] Ch 284 at 318.

3.15 Therefore a matter can be considered to be contained in a public document even where its appeal and concern is only of interest to a small section of the community. As evidence of this Lord Blackburn suggested books of the manor which would be made public documents where they concerned all the people interested in the matter. These were held to be public documents in *Heath v Dunne*.[19]

3.16 Limits were placed on this public document exception in *Heyne v Fischel & Co*.[20] where records maintained by Post Office officials and which listed the times of receipt and dispatch of telegram messages were held not to form public records. This was owing to their not being concerned with public rights, they were held simply for the purpose of regulating Post Office employment figures.

3.17 There must be a public duty on the official to inquire into and record the facts in the documentation.

3.18 The person compiling the documentary statement must be under a public duty to satisfy himself of the truth of the statement and a record created at the behest of a private individual will not suffice as per *Doe d France v Andrews*[21] Data which has not been held sufficient has included entry of marriage registration in a parish register which was held not to be sufficient documentary evidence of the indicia of marriage.

3.19 This condition was found not to have been sufficiently complied with in *Mulhern v Cleary*[22] relating to parochial registers of births, deaths, baptisms and marriages which were not classified as public documents.

(i) The Irish Context

3.20 In *O'Conghaile v Wallace,*[23] the plaintiff attempted to rely on the Prison Rules in his litigation to establish improper treatment at the hands of the prison authorities. The Supreme Court dismissed his claim and held that he had failed to adduce any admissible evidence of the treatment he was entitled to. He produced a document to the court which purported to contain a list of official "Local Prison Regulations" which was not sufficient to be regarded as admissible evidence of a public document.

---

19 [1905] 2 Ch 86.

20 (1913) 30 TLR 190.

21 (1850) 15 QB 756 (Erle J).

22 [1930] IR 649.

23 [1938] IR 526.

3.21 FitzGibbon J noted that to be a public document in evidence for the purposes which the plaintiff had intended, the document would have to attain a standard and bear an official stamp.[24] The document was not adduced as a statutory rule or order and it bore no marking from the Stationary Office or a delegated printer under the auspices of the government printers. Neither was the document offered under the *Documentary Evidence Act 1925* or the *Interpretation Act.* FitzGibbon J found that if there were in fact any prison regulations as had been hinted at, the plaintiff could properly have adduced secondary evidence of the regulations by admitting a copy.[25]

3.22 The issue of whether an entry in a public register can be admitted as proof of its contents was categorically addressed in Ireland in *DPP v McDermott.*[26] The case concerned a prosecution under the *Intoxicating Liquor Acts* on a charge of selling alcohol to a minor. At the trial the prosecution produced the minor's birth certificate as proof of his age. The argument centred on how the prosecution could prove the date of birth of the minor in question where the defendant submitted that there was no proof that the excerpt from the register was the birth certificate of the person in question. They argued that only the mother of the minor could testify as to the date of birth. The statutory provisions involved here went beyond section 5 of the *Criminal Evidence Act 1992* to answer the question of whether a birth certificate was, in and of itself, sufficient to be admissible as proof of the contents. This engaged the *Social Welfare (Miscellaneous Provisions) Act 2002* which amended the *Registration of Birth and Deaths (Ireland) Act 1863* providing for the admissibility of an extract or copy of a document from the register.[27] Section 30A of the 1863 Act, as inserted by the 2002 Act, stated:

> "(2) Every document purporting to be a copy of or extract from an entry in the registers kept under this section shall be received in evidence in any proceedings and shall, until the contrary is shown, be deemed to be a true copy of or extract from the entry and shall be evidence of the terms of the entry.
>
> (3) Evidence of an entry in a register kept under this section may be given by production of a copy of the entry certified by an tArd-

---

24 *O'Conghaile v Wallace* [1938] IR 526.

25 *Ibid.*

26 [2005] IEHC 132.

27 Sections 30A, 30B and 30C were brought into effect by S.I. 269 of 2003 on July 1st 2003. The offence was alleged to have been committed in April 2002, which gave rise to the question whether the amendment was procedural in nature and could have retrospective affect.

Chláraitheoir, an officer duly authorised to act in that behalf or a register and it shall not be necessary to produce the register itself."

3.23 The defendant attempted to argue that strict proof was required and encouraged a restatement of the Best Evidence Rule which would only be satisfied by the testimony of the minor's mother. This assertion was rejected by the High Court which held that a date of birth could be established by the production of a certified copy of a birth certificate where statutory provisions have been complied with and that the document in these circumstances was deemed to be evidence of the terms asserted therein until the contrary was shown.

3.24 The rationale for this is that although the public administrator in question is under a duty to record, the document is only admissible as evidence of the facts that this official was under a duty to record. It is not admissible as evidence of other facts introduced in the document and which fall outside the remit of the public clerk to record. The basis for this is the reasoning in *R v Clapham* where a register of baptisms was held admissible as proof of the ceremony having taken place but not evidence of the date of birth of the child.[28]

3.25 The document must record information of a public matter although it has been held that this need not necessarily be of concern to the whole of the public. Examples include a company's statutory returns in the register which have been held to qualify as significantly 'public' in nature in *R v Halpin*.[29]

3.26 The documentary statement must be created on the expectation that it will be retained - the document must have been created for the purpose of being retained and not on a temporary basis- *Heyne v Fischel & Co*[30]*; Mercer v Dunne;*[31] *White v Taylor.*[32]

3.27 The Commission has already provisionally recommended that the well-established elements of the definition of a public document should be included in the Commission's proposed statutory framework and that this clarified definition of a public document should draw together the relevant principles of the common law.[33]

---

28 (1829) 4 C & P29.

29 [1975] QB 907.

30 (1913) 30 TLR 190.

31 [1905] 2 Ch 538.

32 [1969] 1 Ch 150.

33 See paragraph 1.41, above.

3.28 The Commission now turns to examine some of the detailed requirements that would complement this approach.

B Proof of the Contents of Public Documents

3.29 Proof of the contents of public documents is provided for by a number of statutory provisions which provide for the admission of examined copies, certified copies or Stationary Office-issued copies. Thus, section 5 of the *Documentary Evidence Act 1925* states:

> "Every copy of an Act of the Oireachtas, proclamation, order, rule, regulation, bye-law, or other official document which purports to be published by the Stationery Office or to be published by the authority of the Stationery Office shall, until the contrary is proved, be presumed to have been printed under the superintendence and authority of and to have been published by the Stationery Office."

3.30 The 1925 Act follows the approach taken in many comparable pre-1922 Acts dealing with the admissibility of public documents. The Commission turns to discuss a number of these.

(1) Public Documents Admissible by Statute

3.31 In examining the following pieces of legislation, the Commission does so on the basis that those which have been rendered obsolete by the passage of time and other legislative enactments will be repealed and that the remaining elements will be incorporated into the Commission's proposed legislative framework on documentary evidence.

(a) Evidence Act 1845

3.32 The *Evidence Act 1845* provided for the production as admissible evidence of secondary evidence in the form of certified copies of official and public documents where these are sealed, signed and stamped. There is no need to offer further without proof as to the provenance of the seal or signature attached. This exception extended to public and judicially noticed documents which were acceptable in the absence of the original as prima facie proof of their contents. The main elements of this Act have been included in the *Documentary Evidence Act 1925*.

(b) Evidence Act 1851

3.33 The *Evidence Act 1851* provides a framework through which to obtain access to documents for inspection including extra-jurisdictional proclamations, treaties, judgments and other Acts of State or of foreign states. It accomplished this by permitting copies to be taken for the purposes of

inspection.[34] Under section 7, concerned the admissibility by secondary evidence of proof of foreign and colonial acts of state and judgments which were deemed admissible in the form of an examined copy or a copy authenticated with the seal of the court of the foreign state.

3.34 More significantly, section 14 is a catch-all provision which provides that a document which is of such public nature that it is admissible as evidence on production from custody, and where no statute exists which renders its content provable by a copy, it may be proved by certified or examined copy.

(c) County Boundaries (Ireland) Act 1872

3.35 The *County Boundaries (Ireland) Act 1872* provides that certified copies of ordnance survey maps under the Act or under the *Survey (Ireland) Acts 1854 to 1859* shall be conclusive evidence of the original of the map for all purposes.

3.36 Section 4 of the *County Boundaries (Ireland) Act 1872* provides that each copy of any ordnance maps prepared pursuant to either that Act or the *Survey (Ireland) Acts 1845 to 1859* and professed to be duly certified as a true copy, is acceptable as conclusive evidence of the original map and is effectively admissible to prove the boundary of a county. The 1872 Act was discussed in *Brown v Donegal County Council*[35] where the Supreme Court held that the ordnance map furnished in that case did indeed provide *prima facie* evidence (which had not been contradicted) as to where the county's coastline ended. Griffin J commented on the fortuity which caused the legislation to be considered in the case as the provisions under discussion were otherwise not of a kind "general, fully appreciated." Confusion, he suggested, had grown because many practitioners had:

> "probably heard it stated that ordnance maps are not admissible in evidence; this is no doubt due to the statement of general principle to be found in English text-books to the effect that ordnance maps are not in general admissible as between individuals as evidence of title or otherwise as they do not come under the head of public documents."

3.37 Whilst correct from the perspective of section 14 of the *Boundary Survey (Ireland) Act 1854* which provides that no order made in pursuance of the Act will be taken as affecting the boundary of any land with reference to the title, possession, claim or interest, Griffin J pointed out that the same did not hold true for the specification of the marking out of the boundaries of every

---

34 *Evidence Act 1851*, section 6.

35 [1980] IR 132.

"county, barony, parish etc marked out by the boundary surveyor" for all public purposes. With the advent of the *County Boundaries (Ireland) Act 1872*, a copy of any map mentioned in an order made pursuant to the *Survey (Ireland) Acts, 1854-1859*, or the Act of 1872 and duly certified as a true copy, "is conclusive evidence of the original map for all purposes, and is admissible in evidence to prove the boundary of a county etc."

3.38 Griffin J also offered examples of how such Acts were relevant in prosecutions under the Customs Acts where a duly certified copy of the relevant ordnance map was to be taken as admissible in evidence "to prove the land frontier between the Republic of Ireland and Northern Ireland", and they could also be utilised to provide accuracy as to the dividing lines in arguments as to the nature of the "land frontier which...divides a dwelling-house, a farm-yard, or a street in a village."

(d) Documentary Evidence Act 1868

3.39 The *Documentary Evidence Act 1868* provides that a proclamation, order or regulation by her Majesty, the Privy Council or any Government Department could be proved by production of either a copy of the Gazette in which it was published or a copy printed by the government printer.[36]

(e) Documentary Evidence Act 1882

3.40 Section 2 of the *Documentary Evidence Act 1882* amended the 1868 Act by rendering copies of statutory instruments and ministerial orders printed by the Stationary Office receivable in evidence (stationary office copies). Section 4 of this Act specifically applied these provisions to Ireland.

3.41 Collectively these Evidence Acts (*Evidence Act 1845, Documentary Evidence Act 1868*, *Documentary Evidence Act 1882)* provided that prima facie evidence of a statute could be presented in court by producing a copy of an official publication or designated archive.

(f) Documentary Evidence Act 1895

3.42 The *Documentary Evidence Act 1895* extended the provisions of the 1868 Act, as amended by the 1882 Act, to proclamations, orders and regulations of the Board of Agriculture.

(g) Documentary Evidence Act 1925

3.43 The *Documentary Evidence Act 1925* contains a number of provisions in relation to the proof of the contents of primary and secondary legislation. Section 2 provides that production of a copy of an Act of either

---

[36] *Documentary Evidence Act 1882,* section 2.

House of the Oireachtas printed under the authority of and by the Stationary Office is prima facie evidence of the Act.

3.44 Section 4 provides that evidence of rules, orders, regulations, or bylaws may be given by producing a copy of the Iris Oifigiúil which contains the instrument in question, or by the production of a copy of the instrument printed by and under the authority of the Stationary Office.

3.45 Section 8 provides that the Evidence Acts 1845, 1868 and 1882 do not apply to documents to which the 1925 Act applies, so that these Acts remain valid as they apply to other documents to which the 1925 Act does not apply.

(h) Evidence (Colonial Statutes) Act 1907

3.46 The *Evidence (Colonial Statutes) Act 1907* was an Act to facilitate the entry into evidence of statutes of any British possession.[37] It allows judicial notice to be taken of any Acts, Statutes etc. of the legislature of any British Possession which purport to be printed on Government printers, without requiring proof that they were so printed.

(i) Bankers' Books Evidence Act 1879

3.47 The *Bankers' Books Evidence Act 1879* is discussed in greater detail in Chapter 4 and the Commission notes here that it recommends its retention as a specific regulatory model for a discrete class of documents.

3.48 The *Bankers' Books Evidence Act 1879* sought to avoid the inconvenience which would have been created by the necessity to produce originals of banker's books for the purposes of litigation.

3.49 Section 3 provides that where the book in question is one used ordinarily by the bank, the entry is one made in the ordinary course of business, the book is in the custody of the bank and the copy is examined (as against the original), a copy of an entry into the bankers' book can be received as prima facie evidence of such an entry, and its contents, in all legal proceedings.

3.50 Sections 4 and 5 provide that section 3 requirements can be proved by the affidavit or testimony of a bank official.

3.51 Also under section 5, bankers are non-compellable, except by court order, to produce the bankers' book in order to prove its contents.

3.52 Section 7 provides that any party to a legal proceeding, civil and criminal, can apply for an order that he be at liberty to inspect any entries in

---

[37] A British possession here means a part of the dominions of the United Kingdom.

bankers' books for the purposes of such proceedings, without notice where necessary.

(j) Public Documents in the UK

3.53 Some of the pre-1922 Acts already referred to remain in force in the United Kingdom. These include the *Evidence Act 1845* and the *Documentary Evidence Act 1882*[38] by which proof of Private Acts of Parliament may be given through the production of the Queen's Printer's or Stationary Office copy. Under section 3 of the English *Interpretation Act 1978* every Act is to be considered a public Act to be judicially noticed as such, unless the contrary is expressly provided for by the Act. This means it is unnecessary to produce any hard copy of an Act passed after 1850. Statutory instruments are provable by the production of the gazette containing them.[39]

3.54 Data recorded and held in the Public Record Office is provable by producing copies certified by the Keeper of the Public Records in accordance with the *Public Records Act 1958*.[40] In the case of electronically held the *Public Records Act 1958 (Admissibility of Electronic Copies of Public Records) Order 2001* regulates the area providing for the legal admissibility and authenticity of copies from the Public Record Office website.

3.55 Home Office concerns relating to national security issues are reflected in the provisions of the *Terrorism Act 2000* which provides for the admissibility of notices and directions issued by the Home Secretary under the Act as authentic evidence unless proved otherwise.[41]

3.56 Both in England and Ireland, the *Evidence Act 1845* remains in force. Section 1 of this states that where a statute permits a document to be proved by means of a certified copy, mere production of this certified copy is in itself sufficient evidence to ensure admissibility. For official or public documents which do not have a standing statutory provision permitting their admittance by the production of a copy, section 14 of the *Evidence Act 1851* is applicable and provides a legislative catch-all mechanism. This provides that where a document is public in nature so as to be admissible in proceedings and any question as to its admissibility would be resolved by the mere production of the document released from proper custody then by virtue of section 14 the document may be proved by a certified or examined copy.

---

38 Section 3.

39 *R v Clark* [1969] 2 QB 91 which acknowledged that judicial notice may be taken of a statutory instrument.

40 Section 9.

41 Section 120.

3.57 These Evidence Acts remain in force and despite the passage of time they retain sufficient legislative currency to admit a plethora of documents in which the public have an interest without the need to produce the original before the court.

(2) Evidence of Professional Qualifications

3.58 Section 23 of the *Pharmacy Act 2007* provides for the admissibility as evidence in legal proceedings and authentication of copies of the register of pharmacists as well as certified copies of extracts of this in circumstances illustrated therein[42] where it is shown to bear a signed statement by the registrar that it is such a copy or extract.[43] This evidence is subject to rebuttal but "in the absence of evidence to the contrary, proof of the matters stated".

3.59 Section 5(5) *Criminal Evidence Act 1992* further provides that where a document is tendered which purports to be a birth certificate (issued pursuant to the *Birth and Deaths Registration Acts 1863 to 1987*) purportedly identifying the parentage of the individual, this shall be admitted in any criminal proceedings as evidence indicative of the relationship illustrated therein. Section 11 of the *Criminal Evidence Act 1992* also provides that over the course of any criminal proceedings, evidence of the passage of a resolution of either House of the Oireachtas, be it before or after the commencement of the section, may be given through the production of a copy of the Journal of proceedings of the House in question and as relate to the resolution and purporting to have been published by the Stationary Office.

(3) Judicial Notice

(a) Judicial Notice of Public Documents and Their Admittance in Evidence

3.60 Where for example an official document is judicially noticed this means that facts as to its contents can be admitted in evidence where the fact is so widely known that it cannot reasonably be disputed. Where a document is accepted as being judicially noticed, this mechanism has the effect of dispensing with the need to have a witness to introduce the evidence before the court and the presumption of due execution applies.

3.61 Section 13 of the *Interpretation Act 2005* stipulates that an Act of the Oireachtas is a public document and that mandatory judicial notice must be taken of this fact.

---

42 *Pharmacy Act 2007*, section 23 (b).

43 Section 23 (b)(ii).

(b) Judicial Notice of Domestic Documents and Their Admittance in Evidence

3.62 Examples of judicial notice and the application of this rule of evidence to different documentary materials includes notice granted to appropriately designated bodies under section 48 of the *British Irish Agreement Act 1999.* Under this provision seals and documents issued under these seals are receivable as prima facie documentary evidence unless the contrary is proven.

3.63 Similarly, section 12(3) of the *Civil Registration Act 2004* provides that the Official Seal of the Registrar General shall be judicially noticed.

3.64 Section 13(4) of the 2004 Act provides for the prima facie admissibility of entries of each birth, stillbirth, adoption, death, marriage, divorce decree and nullity in the State. These may be produced to the satisfaction of the court by means of a copy of a document purporting to be a legible copy of the entry certified as a true copy by the Registrar General. Section 68(1) of the 2004 Act provides that an entry in the register of births, deaths and stillbirths is not of itself admissible evidence of the recorded event other than where (a) the entry is signed by the individual who gave the information in relation to the event to the recording registrar, (b) that individual who evidenced the information was required by the 2004 Act (or a statutory provision repealed by the Act) and (c) the entry was made pursuant to the provisions of the 2004 Act or a statutory provision repealed by the Act.[44]

3.65 In accordance with section 68(3), in circumstances where a birth, death or stillbirth is recorded 12 months or more following the date of its occurrence, the relevant entry in the appropriate register will not be evidence of the occurrence unless it purports to have been made with the authority of the Registrar General or an authorised officer of the relevant authority.

3.66 Public documents are admissible as evidence of the proof of their contents which has, as discussed, been provided for by a number of statutory provisions which provide for the admission of examined copies, certified copies or Stationary Office-issued copies offered under the *Documentary Evidence Act 1925*, section 5 of which provides that:

> "Every copy of an Act of the Oireachtas, proclamation, order, rule, regulation, bye-law, or other official document which purports to be published by the Stationery Office or to be published by the authority of the Stationery Office shall, until the contrary is proved, be

[44] Subsection 2 provides that paragraphs (a) and (b) of subsection1 do not apply to (i) an entry in the register of births made pursuant to section 3 of the *Births, Deaths and Marriages Registration Act 1972*, or (ii) an entry in the register of deaths made pursuant to that section or section 41 of the 2004 Act.

presumed to have been printed under the superintendence and authority of and to have been published by the Stationery Office."

3.67 The *Documentary Evidence Act 1925* provides for the admissibility of copies of official documents and public records. It allows for the admittance of copies of these documents as *prima facie* evidence in proceedings without the need for further authenticating evidence where either a copy of the document itself such as an Act of the Oireachtas[45] is in issue or by the production of an official journal or other officially recognised document printed under the auspices or authority of the Stationary Office. Further sections act as a regulatory safety net providing for the admissibility as *prima facie* evidence of "any rules, orders, regulations or byelaws" through the production of the Iris Oifigiúil publishing the State sanctioned version of the official document[46] and extending this courtesy of recognition to those public documents byelaws, regulations and orders made under a British statute.[47]

3.68 The *Documentary Evidence Act 1925* also contains provisions for the admissibility of domestic legislation. Under section 2 an Act of the Oireachtas regardless of its being passed before or after the enactment of the *Documentary Evidence Act*, "may be given in all Courts of Justice and in all legal proceedings by the production of a copy of such Act or Journal printed under the superintendence or authority of and published by the Stationery Office."

3.69 Section 3 of the *Documentary Evidence Act 1925* permits the admission of proclamation orders and other official documents which may be given in "all Courts of Justice and in all legal proceedings" following the production of a copy of the Iris Oifigiúil containing such an Order or proclamation, by the production of a copy of such proclamation, order or other official document itself printed under the superintendence or authority of and published by the Stationery Office; or by furnishing a copy of or extract from such proclamation, order or other official document which has been certified as true by the Secretary to the Government or by some other officer of the Government authorised in that behalf by the Taoiseach.

3.70 The *Documentary Evidence Act 1925* is an Act which regulates the mode of proof of official public documents. Insofar as they affect other types of documentary evidence it did not repeal the *Evidence Act 1845*, the *Documentary Evidence Act 1868* and the *Documentary Evidence Act 1882*,

---

45 Section 2.

46 Section 4 (1).

47 Section 4 (2).

which continue in force.[48] These statutory provisions are for the most part archaic and fragmented in nature. The bulk of the Acts remaining in force are listed by the Office of the Attorney General and which have continuing effect and are schedules in *Statute Law Revision Act 2007*[49] pending repeal and re-enactment in future legislation. They also comprise the lion's share of those statutes specifically put forward as in need of modernisation and consolidation in the Programme of Law Reform as set out by the minister for Justice in 1962.

(c) Judicial Notice of Foreign Documents

3.71 The *European Communities (Judicial Notice and Documentary Evidence) Regulations 1972* provide for the admissibility as documentary evidence of various EC Treaties, of the Official Journal publications[50] as well as any decisions or opinions emanating from the European Court.[51] Prima facie evidence of the contents of these documents is receivable as evidence through the production of secondary copies printed under the superintendence of the Stationary Office or the Official Publications Office.[52] The production of a copy or an extract is also permissible as prima facie documentary evidence where certified by an official of the issuing institution. There is no requirement to supplement the document offered with introductory testimony and the document's verification is not subject to authentication measures such as having to adduce proof of the official's professional capacity or undertaking comparison evidence to verify his handwriting. Due execution is presumed.[53]

3.72 The *Rules of Superior Courts (No. 1) (Proof of Foreign, Diplomatic, Consular and Public Documents) 1999* implemented the 1962 Hague Convention Abolishing the Legalisation of Documents, and thus provides for documents emanating from or destined for use in contracting States subscribing to the Convention to be accepted as documentary evidence before the courts as proof of their contents. This material is accepted without proof and dispenses with other procedural authentication requirements or

> "formal procedures for certifying the authenticity of a signature, the capacity in which the person signing the document has acted, or

---

48 Section 8.

49 Schedule 1 Part 4.

50 Reg. 7.

51 Reg. 4.

52 Reg. 5.

53 Reg. 6 (a).

where appropriate, the identity of the seal or stamp which it bears, be admissible in evidence as such if otherwise admissible."[54]

3.73 While this documentation is admissible as evidence, the trans-jurisdictional nature of the documents is also reflected and section 3 provides a mechanism through which to resolve centrally, any difficulties which may arise in connection with the provenance of the documentary evidence. An application may be made under section 3 in accordance with Article 4 of the Convention. Under this mechanism States are responsible for setting up a Central Authority to resolve any difficulties surrounding documentation issuing from that State. This mechanism requires that the Central Authority from the issuing State to provide particulars as to the way in which the impugned document has been produced and vouch for the "authenticity of the signature, the capacity in which the person signing the document has acted, or the identity or seal of the stamp which it bears".[55]

3.74 In compliance with the provisions of the Convention, documents executed by diplomatic or consular missions are admissible in evidence without further proof in foreign courts.[56] Provisions are likewise made for the receipt as documentary evidence of data materials executed in accordance with notarised, apostillised instruments as a means of proof for foreign public documents. This vouches for the proof of the documents which is admissible as evidence of the proof of its contents.[57]

3.75 When it comes to circulating and exchanging documents produced in litigation in another jurisdiction, the interaction of these documents can be accommodated in accordance with the *1965 Hague Convention on the Service Abroad of Judicial and Extra-Judicial Documents in Civil and Commercial Matters*. This Convention dictates the procedures to be followed by signatory States in relaying documents relating to proceedings in their national courts for use in foreign courts or tribunals. This Convention was originally implemented in Irish law in 1994.[58]

---

54 Reg 2.

55 *Ibid,* section 3.

56 *Ibid*, section 53.

57 *Ibid,* section 54 (1) and (2).

58 S.I. No. 101/1994. See now the *Rules of the Superior Courts (Service of Proceedings (Regulation (EC No. 1393/2007)) 2009*.

(4) Public Records and Reports

3.76 The United States has again taken the initiative in formally legislating for the admissibility of public records and reports which include record management and compilation systems (in any form), of public offices or agencies which clarify the activities of a public office or agency, or identify any "matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law", are admissible unless there is a risk that the information indicates a lack of trustworthiness.[59]

3.77 In the United States, where electronic documentary evidence has been commonplace for years, the federal Court of Appeals for the Ninth Circuit decided in 1979 that electronic documents were acceptable in evidence as public documents. In *United States v Orozco*[60] it was held that certain government computer records could be drawn within the public records exception to the hearsay rule and were properly admissible as documentary evidence. Later cases have expanded the concept of government electronic records as fitting within the scope of public documents. These include *US v Thomas*[61] and *Hughes v US* which held that Internal Revenue Service documents which had been generated by the computer were admissible as public documents.[62]

(5) Absence of Public Record or Entry

3.78 This exemption and provisions accommodating public documents serve to admit evidence, in the form of a certification or testimony to the same effect, that diligent search failed to disclose the disputed document.

3.79 Records affecting an interest in property may also be admitted as public documents purporting to record the establishment of an interest in property may be adduced in satisfaction of proof of the contents of the originally recorded document as well as proof of its due execution and evidence of the chain of custody where the instrument itself is a record of a public office and an applicable statute authorises the recording of documents of that kind in that office. Statements in documents affecting an interest in property are also

---

59 Federal Rules of Evidence 803 (8).

60 590 F .2d 789, (9th Cir.) at 793-94.

61 78 AFTR .2d 52 96 (9th Cir.).

62 953 F .2d (9th Cir. 1992) at 540.

included where the issue stated was relevant to the purpose of the document, unless changes have taken place in relation to the property since the document was executed and which have revealed an inconsistency with the truth of the document.

(6) Statements in Ancient Documents

3.80 Ancient documents are those documentary statements in existence twenty years or more and the authenticity of which is established by their vintage and the fact that they have remained uncontested for a specified period (20 years).

(7) Conclusion on Public Documents

3.81 The long-standing approach in various pre-1922 Acts dealing with public documents is that they are presumed to be admissible. This has been confirmed in legislation enacted since the foundation of the State, beginning with the *Documentary Evidence Act 1925* and including recent legislation such as the *Pharmacy Act 2007.* In view of this, the Commission has concluded that, in general (and as an exception to the exclusionary rule for hearsay evidence), a public document, defined in the manner already provisionally recommended by the Commission, should be presumed to be admissible as proof of its contents, subject of course to any contrary evidence as to its authenticity.

3.82 *The Commission provisionally recommends that, in general (and as an exception to the exclusionary rule for hearsay evidence), a public document, defined in the manner already provisionally recommended by the Commission, should be presumed to be admissible as proof of its contents, subject to any contrary evidence as to its authenticity.*

C Private Documents

3.83 The position is very different as regards private documents, where proof of due execution is not presumed and the production of a copy would not suffice to have the document admitted in evidence. Therefore proof of due execution, attestation, handwriting or signature will be required. This may be satisfied in a number of different ways, for example, by oral evidence from the author, signatory or one who witnessed the signing or writing of the document. In the alternative an admissible hearsay statement of the author or a witness may suffice to authenticate the evidence.

3.84 The statutory provisions and exceptions which stretch to enable public documents to be accepted as admissible evidence have the knock-on effect of dispensing with the necessity of having to satisfy the court that the documents in question have been properly executed.

(1) Proof of Handwriting

3.85 Where it is intended to produce a private document in proceedings the court will require that evidence be advanced to show that the private document has been duly executed. Due execution will be established by showing that the document was signed by the person who purported to so sign in order to go towards establishing the reliability of such a document. This can be undertaken by showing proof of the handwriting or signature be it a manual signature or electronic signature.[63] These requirements will be dispensed with where it can be established that the document in question is more than 20 years old and has come from a verifiable and properly maintained custody. From this the court will be entitled to infer formal validity. Proper custody in these circumstances means custody which is reasonable based on the circumstances arising in the case and does not necessarily imply the most appropriate custody which is available.[64]

3.86 When it comes to proving traditionally hand-executed documentary evidence, proof of handwriting can be undertaken. This can involve calling oral testimony of the person who is put forward as having written he document or signature in question. This may be accomplished by producing a statement (a hearsay statement) of the person to that effect. Otherwise, testimony or a written statement (most likely of hearsay information) may be offered to the court from someone who saw the document attested or executed.[65]

(2) Comparison

3.87 Comparison techniques are also used to verify handwriting and signatures affixed to documentary evidence. It has been argued that all attempts to verify a signature or handwriting are variations on the theme of comparison. In the English case *Doe d Mudd v Suckermore*[66] it was noted that "all evidence of handwriting is in its nature comparison. It is the belief which a witness entertains on comparing the writing in question with an example in his mind derived from previous knowledge."[67]

3.88 Comparison techniques might suggest the need for expert testimony but, in fact, non-expert, familiarity comparison of two documents is also

---

63 See further Chapter 7.

64 *Bishop Meath v Marquess of Winchester* (1836) 3 Bing NC 183.

65 An early example of this as a non-contested means of proving a signature is *Jones v Jones* (1841) 9 M & W 75.

66 (1837) 5 Al & El 703.

67 *Ibid,* at 739.

permissible. The comparison undertaken will affect the weight of the evidence. There is also the possibility that the documents may be submitted to the court for adjudication on shared characteristics of the two documents. In *R v Stephens,*[68] a New Zealand case, this procedure was, however, rejected as inappropriate and it was held that external evidence to prove the writing must be offered.

(3) Opinion

3.89 Opinion evidence may also be offered as to the status of the signature. This may be offered by a witness who did not observe the act of singing but who is sufficiently acquainted with or associated with the signature or handwriting in question. This means of identification has long been recognised.[69] Where proof of verification is achieved in this way, it will impact on the evidential weight of the document as noted by Denman CJ in *Doe d Mudd v Suckermore*.[70]

3.90 This is also true of voice recognition technologies and opinions based on the comparison of audio voice recordings with human knowledge of a familiar voice.

3.91 A stipulation when offering opinion testimony is that the witness must be sufficiently acquainted with the writing or signature he or she is to identify so that essentially the evidence goes beyond the witness's opinion and is really based on his or her reputed knowledge. In the Canadian case *R v Pitre,*[71] the witness's knowledge, having previously seen two letters and two postcards allegedly by the same hand, was deemed unsatisfactory to make the witness sufficiently versed in the author's handwriting.

(4) Other presumptions attaching to private documents

3.92 There is a presumption that the document was generated on the date on which it purports to have been created. There is also a corollary that presumes that any alterations on the face of the document were made prior to execution. This presumption, however, does not extend to wills where, instead, the onus rests on the person who seeks to derive an advantage from an alteration in the document and who therefore must adduce evidence to establish that the alteration was made before the will was executed. Proof of due execution is also dispensed with where a party, on whom a notice to

---

68 [1999] 3 NZLR 81.

69 *Lewis v Sapio* (1827) Mood & M 39.

70 (1837) 5 Al & El 703 at 750.

71 [1933] 1 DLR 417.

produce documents has been served, refuses to produce the original in his or her custody.

3.93 The rationale behind rules as to the proof of such documents is to alleviate the burden on parties, in particular to avoid mounting expenses or inconvenience in trying to establish their authenticity. The Commission has concluded that this well-established distinction between private and public documents, in which there is no presumption of due execution of private documents, should be maintained and that this should be placed on a statutory footing.

3.94 The Commission provisionally recommends that the well-established distinction between private and public documents, in which there is no presumption of due execution of private documents, should be maintained and that this should be placed on a statutory footing.

CHAPTER 4 BUSINESS DOCUMENTS AND THE BUSINESS RECORDS EXEMPTION

4.01 In this Chapter, the Commission examines business documents as another of the main exceptions to the exclusionary rules of evidence in their application to traditional and now electronic documentary evidence. Part A attempts to define a business record as a means by which to admit secondary evidence in the form of a copy or extract of the records of data maintained, received or generated in the course of business.

4.02 Part B examines documents which are generated in anticipation of litigation and recommends their continued exclusion from evidence as records (owing to the possibility that they have been contrived rather than produced spontaneously as part of the every-day operation of the business) other than where a specific legislative provision permits and regulates their admission in evidence.

4.03 Part C focuses on a particular aspect of this exemption - the bankers' books exception, regulated by statute and which the Commission provisionally recommends ought to be retained. This Part discusses the extent of a "document" when held electronically or otherwise by a financial institution and how such documents are in fact "kept" by the institutions in question.

4.04 While discussing the legislation in this area, beginning with the *Bankers' Books Evidence Act 1879*, in Part D the Commission considers the purposes for which this legislation is still required for example for the detection and prevention of fraud and money laundering and discusses the domestic and extra-territorial nature of these legislative provisions for the purposes of adducing and admitting documentary evidence. The Commission concludes that the business/bankers' books exemption to the exclusionary rules should be retained in the Commission's proposed legislative framework.

A Business Documents Admissible as an Exception to the Exclusionary Rules of Evidence

4.05 Business records, or at least specific examples of them, present a further exception to the exclusionary rules. Specific legislation has, since the 19th Century, been enacted to eliminate any difficulty associated with proving facts in cases of commercial litigation before the courts. In these instances,

documents such as those retained by banks and other financial institutions, are received on the basis that they have been shown to be presumptively accurate.

(1) Defining a Business Record

4.06 In acknowledgment of their voluminous and repetitive nature, most jurisdictions have statutory exceptions to the Hearsay Rule to facilitate the admission in legal proceedings of reliable statements contained in "bankers' books" however kept or produced as evidence of the matters recorded. The best-known of these Acts, the *Bankers' Books Evidence Act 1879*, (which continues – with amendments - to apply in Ireland) provides that proof of bank and other business accounting records are presumptively admissible without the need to compel, as witnesses, employees of the bank to prove issues specific to particular accounts, and without causing the bank the inconvenience of physically removing records from their premises.[1]

4.07 Since the enactment of the 1879 Act, financial services and business generally has obviously undergone enormous change and expansion. For this reason, specific pieces of legislation providing for the admission of documentary evidence have not been confined to "bankers' books" but have been expanded to include "business records." Thus, the provisions on the admissibility of documentary evidence in the *Criminal Evidence Act 1992* apply to all business records, and section 4 of the 1992 Act defines "business" as including: "any trade, profession or other occupation carried on, for reward or otherwise."

4.08 In the Commission's view, the wider approach taken in the 1992 Act, by comparison with the narrow approach of the 1879 Act, ought to be applied generally. Indeed, the Commission also considers that it could be expanded further to include, for example, "charitable organisation" as defined in section 2 of the *Charities Act 2009.* The Commission considers that this approach should be adopted within the proposed statutory framework for documentary evidence and should apply to both civil and criminal proceedings.

4.09 The Commission provisionally recommends that the proposed legislative framework on the admission of documentary evidence should provide that "business records" should be presumed to be admissible in evidence, that the term should include those business records referred to in the Criminal Evidence Act 1992, namely records kept by "any trade, profession or other occupation carried on, for reward or otherwise" and that the term should also

---

[1] Prior to the 1879 Act, the inconvenience of producing books of the Bank of England had led English courts to accept copies and extracts from that Bank's books without requiring production of the original documents, and the 1879 Act was enacted to provide other banks with the same facility.

encompass records kept by a "charitable organisation" as defined in the Charities Act 2009.

4.10 Additional issues surround the "chain of custody" of a document, including whether a document has emerged from a long drafting process and passed through a chain of intermediaries and is then sought to be adduced in court and whether all these draft steps have been received and generated in the course of trade.

4.11 The Commission acknowledges that while business records should be admissible based on the probability of trustworthiness, it is also keenly aware of the need for legislatively entrenched safeguards. Safeguards would ensure the authenticity, and ultimate reliability, of the evidence provided.

4.12 These safeguards would serve to restrict admissibility to statements made in good faith by persons who knew the subject-matter of their statements and had a strong incentive to be accurate in their recording information in documents which are generated for business purposes. Business records are those which are deemed sufficiently integral to the running of the everyday operation of the business to have been mundane rather than contrived and are admitted in evidence on that basis.

4.13 Indeed such statements may often be more reliable than oral evidence where contemporaneous to the events recorded logging unexceptional daily occurrences where oral testimony can be expected to be patchy and inaccurate, informed by fallible human memory.

4.14 This should not be seen as promoting a supposition that the document should be prima facie evidence of proof of its contents, but merely that it be admissible as evidence. The documentary statements must still pass over evidential hurdles including that it be shown to be relevant and have sufficient integrity. Such evidence is also amenable to challenge on the grounds that the person who presents it is open to challenge as to his credibility and his personal knowledge and the credibility of this person will also speak to the weight of the documentary evidence. The Commission sets out its conclusions on this below.

4.15 The Commission provisionally recommends that business documents be accepted as admissible evidence if the document was created or received in the course of a business and where:

a. The information in the statement is derived from a person who had, or may reasonably be supposed to have had, direct personal knowledge of that information;

b. That the documentary statement has been produced for the purposes of a business; and

c. That the information is contained in a document kept by a business.

B The Retention of Documents and Records in Anticipation of Litigation

(1) Admissibility of Documents Generated in Anticipation of Litigation Ireland

4.16 The recommendations already made by the Commission concerning business documents are limited to records created in the ordinary course of business. It is clear that an inclusionary approach can be taken to these documents because they are deemed to be created for the benefit of the business with no incentive for anything other than accuracy. Business records based on anticipation of litigation (in some States referred to as being made in precognition of litigation) are usually dealt with differently. The Commission now turns to examine this category of business records.

4.17 Section 5 (3)(c) of the *Criminal Evidence Act 1992* provides that documents generated in anticipation of litigation are inadmissible. The Commission considers that this provision should be retained in its current form in the proposed legislative framework, but that a facility could be included to allow certain types of such documents to be admitted. The Commission considers that certain records generated, for example, for the purposes of compliance with occupational safety and health legislation (notably, the *Safety, Health and Welfare at Work Act 2005*) may, by their nature, be produced and generated with the dual aim of regulatory compliance and with a view to possible future litigation, primarily civil litigation but also increasingly criminal proceedings under the relevant legislation. This dual purpose was recognised by the UK House of Lords in *Waugh v British Railways Board,*[2] in which it was held that the compliance element prevented such records from being subject to legal professional privilege, even though they may have been prepared with litigation partly in mind, a view which has been followed by the Irish courts.[3]

4.18 The law has already recognised the impracticality of such a strict adherence to rule excluding documents on this basis. Thus, section 5 (b)(iv) of the *Criminal Evidence Act 1992* acknowledges the necessity of allowing in records generated by medical personnel when they are adduced as medical records in a criminal trial.

---

2 [1980] AC 521.

3 See, for example, *Silver Hill Duckling Ltd v Minister for Agriculture* [1987] ILRM 516.

4.19 It should be noted that the documentary statements in question relate only to those which are documentary hearsay statements rather than to documents generated and reproduced in legible format but which originate from a computational or digital device. These latter records do not constitute hearsay.

4.20 The *Criminal Justice Act 1994*, which deals with fraud offences, including money laundering, provides for the admissibility of documentary evidence, bodies and financial institutions designated under the 1984 Act[4] who are required to retain copies of all materials used to identify a customer or proposed customer for at least 5 years after the relationship with the person has ended and transaction records for a period of at least 5 years following execution of the transaction.[5] Failure to comply is an offence under the 1984 Act.

4.21 These documents are created and held in situations which anticipate litigation and as such do not strictly come within the confines of admissible documentary evidence under section 5 (a) of the *Criminal Evidence 1992*.

4.22 The financial entities in question are under a duty to retain the original documents or copies, which are then admissible in legal proceedings as evidence of transactions although the stated end usage of these retained records is clearly one of evidence in money laundering proceedings. The burden of maintaining a large volume of this type of documents is recognised and the information may be stored on microfilm or computer software.[6]

4.23 Wire transfer transactions are acknowledged as being particularly vulnerable to money laundering techniques, so the names and addresses of those sending and receiving electronic payment must also be kept for a period of 5 years. Records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account and kept for a minimum of 5 years.

---

4 See section 32(1) of the 1984 Act.

5 Section 32(9)(a) and (b).

6 It is recognised that credit institutions will usually have standard procedures which seek to reduce the volume and density of records that have to be stored while seeking to comply with statutory requirements. Section 131(d) of the *Central Bank Act 1989* extended the definition of "Bankers' Books" in the *Bankers' Books Evidence Act 1879* to include any records in the ordinary business of a bank, kept on microfilm, magnetic tape or in any non-legible form (by the use of electronics or otherwise) which is capable of being reproduced in a permanent legible form.

(2) Concluding Remarks Documents Produced in Anticipation of Litigation.

4.24 An essential principle contained in the *Criminal Evidence Act 1992* is that the information sought to be introduced in evidence was compiled in the ordinary conduct of a business. Therefore the law requires that documents will not be accepted where merely generated in contemplation of litigation, as this may be though to avoid the rule against hearsay. This recognises the enormous probative force of documentary evidence where forming part of the ordinary course of business. The 1992 Act does not grant an unfettered right to submit a documentary record of a trade or business transaction merely because the producing party wishes to avoid the expense or delay of calling the supplier of fact as a witness. If the supplier of the relevant information is identifiable, within the jurisdiction and can reasonably be supposed to remember the relevant matters, the propounding party has no discretion to submit documentary evidence in his or her place.

4.25 On the basis of this discussion, the Commission has provisionally concluded that statements produced in anticipation of litigation ought to remain inadmissible as evidence of matters which they contain, except in certain stated exceptions, such as those involving money laundering as already provided for in the *Criminal Justice Act 1994*.

4.26 The Commission provisionally recommends that statements produced in anticipation of litigation ought to remain inadmissible as evidence of matters which they contain, except in certain stated exceptions, such as those involving money laundering as already provided for in the Criminal Justice Act 1994.

(3) Admissibility of Documents Generated in Anticipation of Litigation in Victoria (Australia)

4.27 The updated and integrated Uniform *Evidence Act 1995* as incorporated for instance in the Victorian *Evidence Act* 2008 has been informed by the developing case law in the area of documents produced in anticipation of litigation which served to limit the expansion of the business documents exception to information which is kept in an organised form accessible in the usual course of business. [7] It is further limited to data which comprises the internal records in of the company's business as identified in *Atra v Farmers & Graziers Co-op Cp Ltd*[8] which confirmed that documents are not excluded automatically where they may be of use in legal proceedings. It is only where

---

7 *Karmot Auto Spares Pty Ltd v Dominelli Ford (Hurstville) Pty Ltd* (1992) 35 FCR 560, at 565.

8 (1986) 5 NSWLR 281, at 288.

the documents are purposefully generated for litigation and where litigation is in the mind of the author of the document[9] or where the prospect of legal proceedings played "some part in the decision to prepare" the documents in question.[10]

4.28 The question of whether an article in the journal of association of mushroom growers was admissible as a business record was discussed in *Roach v Page (No 15).*[11] Sperling J held that it did not qualify as a business record because it did not record data of the activities of the business. The records in question were products of the business, not a record of its business activities generated in the ordinary course of the business.

4.29 The Australian courts have considered this element of the admissibility of documents in evidence in some detail. The Australian courts have held that the decisive factor is not the timing on the document and that the therefore it is not a question of whether the document is generated contemporaneous to the litigation being pursued as suggested by Maurice J in *S and Y Investments (No 2) Pty Ltd v Commercial Union Assurance Company of Australia Ltd.*[12]

4.30 The mere contemplation of litigation is not sufficient to exclude the documents in question from evidence and proceedings must be probable though need not necessarily been instituted. This was the case in *Creighton v Barnes*[13] the principle of which was approved by *Nikolaidis v Legal Services Commissioner.*[14]

C The Bankers' Books Exception in Ireland

4.31 Where a business record is adduced to establish the proof of its contents the law has moved beyond requiring the person who initially generated the document to be available for cross-examination. This has resulted in the development of the so-called "shop-book" rule which makes business and banking records directly admissible.

---

9 (1986) 5 NSWLR 281, at 290.

10 *Timms v Commonwealth Bank of Australia* [2003] NSWSC 576 at 15.

11 [2003] NSWSC 935.

12 (1986) 82 FLR 130 at 152.

13 NSW Supreme Court 18 September 1995, BC 950786 at 2.

14 [2007] NSWSC 130 by Beazley JA at 61.

4.32 The *Bankers' Books Evidence Act 1879* has been amended on a number of occasions since the foundation of the State, including by the *Bankers' Books Evidence (Amendment) Act 1959,* which facilitates the proof of banking transactions in evidential terms, and the *Central Bank Act 1979* which provides for some technological updating of the definition of "bankers' books". The *Bankers' Books Evidence Acts* have been described as involving a statutory erosion of the banker's duty of secrecy[15] and a legislative means by which to compel disclosure of client account details in litigation to which the bank is not a party.

4.33 The *Bankers' Books Evidence Act 1879* as amended facilitates the proof of banking transactions without the need to produce the original documentary evidence relied upon. The Act greatly benefits litigants as it enables a party to procure documentary evidence from the bank by allowing any party to legal proceedings to apply to the Court for permission to inspect and to take copies of such entries for the purposes of such proceedings.[16] This has a knock on impact on the third party duty to disclose documents on what would otherwise be an opaque transaction. The 1879 Act in effect mandates discovery so as to enable the inspection and admissibility of the accounts of a person or financial entity not a party to the proceedings while the ordinary rules of discovery and inspection apply between the parties.[17] A further far-reaching effect of the 1879 Act, as amended, is that copies of documents not ordinarily admissible of themselves are made admissible as *prima facie* evidence of the matters recorded in them.[18] This creates an exception to the hearsay rule for the documents to which the 1879 Act applies.[19]

4.34 *The Bankers' Books Evidence Act 1879* provides the means by which banks may provide documentary evidence to requesting tribunals. Sections 3 to 6 of the 1879 Act, as amended, set out the formula for the production of these bankers' books while avoiding the usual procedural requirements.

4.35 Section 3 of the 1879 Act provides:

> "Subject to the provisions of this Act, a copy of any entry in a Banker's Book shall in all legal proceedings be received as prima

---

15 Donnelly, M. "*The Erosion of the Bankers' Duty of Secrecy*", (1996) 3(9) CLP 226.

16 Section 7 of the 1879 Act.

17 *Waterhouse v Barker*, [1924] 2 KB 759; [1924] All ER Rep 777 CA.

18 It is less certain of whether the non-existence of any entry in a banker's book constitutes corresponding evidence of the non-existence of the alleged account or transaction as per *Douglass v Lloyds Bank, Ltd.* (1929), 34 Com Cas 263.

19 See *Harding v Williams* (1880) 14 Ch D 197.

facie evidence of such entry, and of the matters, transactions and accounts therein recorded."

4.36 Section 4 of the 1879 Act states:

> "A copy of an entry in a Banker's Book shall not be received in evidence under this Act unless it be first proved that the book was at the time of the making of the entry, one of the ordinary books of the bank, and that the entry was made in the usual and ordinary course of business, and that the book is in the custody and control of the bank. Such proof may be given by a partner or officer of the bank and may be given orally or by an affidavit sworn before any commissioner or person authorised to take affidavits."

4.37 Section 5 of the 1879 Act, as originally enacted*,* provided:

> "A copy of an entry in a Banker's Book shall not be received in evidence under this Act unless it be further proved that the copy has been examined with the original entry and is correct. Such proof shall be given by some person who has examined the copy with the original entry, and may be given either orally or on affidavit sworn before any commissioner or person authorised to take affidavits."

4.38 Section 5 of the 1879 Act, as amended by section 131 of the *Central Bank Act 1989,* now contains a notable textual updating to reflect changing technology (at least to the late 1980s) and now provides:

> "(1) A copy of an entry in a banker's book shall not be received in evidence under this Act unless it is further proved that—
>
> (a) in the case where the copy sought to be received in evidence has been reproduced in a legible form directly by either or both mechanical and electronic means from a banker's book maintained in a non-legible form, it has been so reproduced;
>
> (b) in the case where the copy sought to be received in evidence has been made (either directly or indirectly) from a copy to which paragraph (a) of this section would apply:
>
> (i) the copy sought to be so received has been examined with a copy so reproduced and is a correct copy, and
>
> (ii) the copy so reproduced is a copy to which the said paragraph (a) would apply if it were sought to have it received in evidence;
>
> (c) in any other case, the copy has been examined with the original entry and is correct.

(2) Proof to which subsection (1) of this section relates shall be given—

(a) in respect of paragraph (a) or (b)(ii) of that subsection, by some person who has been in charge of the reproduction concerned,

(b) in respect of paragraph (b)(i) of that subsection, by some person who has examined the copy with the reproduction concerned,

(c) in respect of paragraph (c) of that subsection, by some person who has examined the copy with the original entry concerned,

and may be given either orally or by an affidavit sworn before any commissioner or person authorised to take affidavits."

4.39 Under these provisions of the 1879 Act, as amended, where the book entry produced by the bank is one of the ordinary book entries maintained during the activities of the bank and is in the continuing custody of the bank and where the entry was made in the ordinary course of business and a copy has been made available and examined against the original in the custody of the bank, the copy or extract of the banker's book is admissible as *prima facie* evidence in legal proceedings. This makes documentary evidence in the form of such business records admissible not only as evidence of proof of themselves but also as rebuttable proof of the facts contained in them. This attaches a probative value to bank records which is acceptable in that it is the grant of a privilege to financial institutions on the assumption that they reliably maintain records in much the same manner as the records of a public body.

(1) Business Records Exemptions in the United States

(a) Admitting Business Records as Electronic Hearsay from a US Perspective

4.40 Under US federal law, hearsay is not generally admissible in a Federal court except as provided by the Federal Rules of Evidence, which were adopted in 1975, "or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress."[20]

4.41 Exceptions are enumerated in Rule 803 of the Federal Rules of Evidence and are particularly relevant to computer printouts. These exceptions mean that evidence in electronic form is not automatically excluded by the hearsay rule, even where the declarant may be available to act as a witness. The means by which to authenticate documentary evidence for the purpose of admissibility are now briefly discussed.

---

[20] Federal Rule of Evidence 802.

4.42 While these are broadly similar to those of other jurisdictions, the Commission examines the US Code Title 28, S 1732 (commonly known as the *Business Records Act*) which provides for admissibility of copies or reproductions of original records produced in the regular course of business. This section states:

> "If any...department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation or combination thereof, of any act, transaction, occurrence, or event, and in the regular course of business has caused any or all of the same to be recorded, copied, or reproduced by any...process which accurately reproduces or forms a durable medium for so reproducing the original, the original may be destroyed in the regular course of business unless its preservation is required by law."

4.43 This elevates the status of any copy to the position previously enjoyed only by an original to such an extent that it countenances the destruction of an original and envisages its replacement with a copy. This copy is sufficient to satisfy any evidential requirements thrown up by the Best Evidence Rule. Under US law such a reproduction, when satisfactorily identified, is as admissible in evidence as the original itself in any judicial or administrative proceeding but also acknowledges the position of the original. This therefore is only to the extent that the introduction of a reproduced copy of the document "does not preclude admission of the original". This has now been incorporated into the Federal Rules and can be found as Federal Rule of Evidence 803 (6) which closely parallels the *Business Records Act*.

(b) Rule 803(6)

4.44 Rule 803(6) of the Federal Rules of Evidence contains a "business records" exception to the hearsay rule and, as with other comparable provisions, it operates as a means to admit as evidence business records, including those kept on electronic devices. Many of the 50 US states have also adopted a comparable business records exception as part of their own state evidentiary rules or relevant statutes. Indeed, a similar business record exception or "shop-book" exception to the hearsay rule had been recognised under US common law. This approach, as in the other common law jurisdictions already discussed, attempted to reconcile the clear importance of business records in litigation against the massive expenses to be incurred which the proponent would be required to overcome should they be required to call every person who had made an entry in a business ledger to offer oral testimony.

4.45 Early judicial opinion in the US seemed focused on assigning a high degree of presumptive reliability to documents contained in or generated through electronic processes. One such approach was to consider the

authenticity of business records on a computer as effectively immaterial, and to treat the records as if they had been kept on paper. In *Vela* and *US v DeGeorgia*[21] the Court of Appeals for the 9th Circuit confirmed that for the purposes of authentication it is of no relevance to the court that the document is or was at one time in electronic form. This view gained considerable force with the Court from the late 1960s, and thus computer printouts produced in the course of business had at least a *prima facie* sense of reliability.[22] However, as time passed and more experience was gained which allowed for a better understanding of the exigencies of computer documents, a more cautious approach crystallised which called for a more secure footing to form the foundation prior to admitting the impugned electronic documents of computer systems in evidence.

4.46 Rule 803(6) of the Federal Rules of Evidence codified the "shop-book" rule as the hearsay exception for "Records of Regularly Conducted Activity." The rule was comparable with the "bankers' books" and business records exceptions in English and Irish law. Rule 803(6) thus permits the admission of data compiled by an individual with knowledge and who has kept the information arising from the regular course of a generally conducted business activity, unless the source of information or method of preparation indicates a lack of trustworthiness.

4.47 The US courts gradually began to treat computer records largely as presumptively trustworthy and admitted them without any need to establish any special foundation by which to determine their authenticity. This progressed to the situation as found in *US v Vela*, discussed above. Offenbecher, citing the decision in *US v Linn*,[23] noted that the Court of Appeals interpreted the "trustworthiness" qualification as having been incorporated into Rule 803(6) as an implied authenticity requirement.[24] This led the Court to regard computer records as effectively authentic unless the opposing party challenged the records as untrustworthy. Offenbecher noted that this "essentially shifted the burden of disproving the authenticity of the records to the opponent." Thus, in the absence of evidence to the contrary to show that they were untrustworthy,

---

21 420 F .2d 889 (9th Cir. 1969) at 893. See also *US v Cestnik* 36 F .3d 904 (10th Cir. 1994) at 909.

22 *US v Dioguardi* 428 F .2d 1033 (2d Cir. 1970) at 1038.

23 880 F .2d at 209 (9th Cir. 1989).

24 Offenbecher, C. *Admitting Computer Record Evidence After In Re Vinhnee: A Stricter Standard for the Future?* 4 Schidler Journal of Law Commerce and Technology 6, 17th October 2007.

the records were admitted.[25] As of 2007, many US courts still interpreted the text of Rule 803(6) to "effectively incorporate an authentication requirement."[26]

4.48 Reliance on this has not always been successful however and courts will limit the interpretation of a business record. In *Monotype Corp. Plc v International Typeface Corp.*, the plaintiffs relied on the business records exception to attempt to admit two e-mails as evidence and which were claimed by the defendants as having infringed their copyright. The court refused to admit the e-mails on ground of the prejudicial nature of the communications and also as they were not created "in the regular course of (the third party's business)."[27]

(2) The Position of Business Documents in England

4.49 If a document forms part of the records of a business or public authority it is admissible without further proof. Section 9 deals expressly with the proof of documents which form part of the records of a business or public authority incorporating the old exceptions into modernised legislation. A business can be taken to include any activity regularly carried out over a period of time, whether for profit or not, by any body (whether corporate or not) or by an individual. A particular document will be taken to be a business record on production of a certificate to that effect signed by any person occupying a responsible position in relation to the relevant activities of the business or authority over its records.

4.50 Section 9 of the *Civil Evidence Act 1995* states:

> (1) A document which is shown to form part of the records of a business or public authority may be received in evidence in civil proceedings without further proof.
>
> (2) a document shall be taken to form part of the records of a business or public authority if there is produced to the court a certificate to that effect signed by an officer of the business or authority to which the records belong.

4.51 Section 9 reserved a general power to the court to ignore all or any of its provisions, which serves to preserve judicial discretion when admitting evidence.

---

25 Offenbecher, C. *Admitting Computer Record Evidence After In Re Vinhnee: A Stricter Standard for the Future?* 4 Schidler Journal of Law Commerce and Technology 6, 17th October 2007.

26 *Ibid.*

27 43 F.3d 443 (9th Cir. 1994).

4.52 For the purposes of manageability, a “document" has a wider meaning than it previously had at common law. It encompasses anything in which information of any description is recorded. A “copy” means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.[28]

4.53 The effect of section 9 is that records made in the course of business are admissible as evidence at the discretion of the Court. This section has gained significance as automatic computer record-keeping systems become increasingly common in an age of vast data-storage and in consequence to the proliferation of newly paper-less offices in the changing work dynamic of the technological age.

(a) Business or Public Documents Containing Documentary Hearsay under the Civil Evidence Act 1995

4.54 Following the enactment of the *Civil Evidence Act 1995*, hearsay evidence is no longer necessarily inadmissible on the sole ground that it is hearsay. In place of a blanket ban, certain safeguards and procedures were put in place to marshal the introduction of hearsay evidence not falling within common law exceptions. On a broad examination, the Hearsay Rule has thus been abolished in its application to documentary evidence. To the extent that many of the tenets of the law against hearsay (both common law and as modified by statutes still in force) remain, its position has been severely diminished.

4.55 A party wishing to adduce hearsay evidence not covered by an existing exception shall give:

(a) Such notice that hearsay evidence is to be adduced “as is reasonable and practicable in the circumstances” to enable matters arising from its hearsay nature to be dealt with.
(b) On request, such particulars as are, similarly, “reasonable and practicable”.

4.56 Yet failure to give this notice does not automatically invalidate the evidence as inadmissible. Instead this impacts on the weight afforded it which in turn may be reflected in costs or other sanctions imposed by the courts. If the maker of the statement is not called by the party adducing the evidence, another party may, with leave, call the maker and cross-examine as if the hearsay statement were evidence in chief under section 2 *Civil Evidence Act 1995*. If the maker is not called at all, evidence detracting from or supporting credibility may still be led.

---

[28] Section 9 (4).

4.57 The *Civil Evidence Act 1995* altered the focus in determining admissibility shifting it from the legal admissibility of electronic documents to the evidential weight of them. It made it easier to prove the authenticity of documents through production of the original or a copy, irrespective of the number of removes between the original and the copy in question.

4.58 Section 9 of the *Civil Evidence Act 1995* permits documents which fall squarely within its definition to prove themselves. It dispenses with the potentially open-ended process of prior authentication otherwise necessary to prove a statement in documentary form. This stems, as with the rationale for simplifying all public and business documents and permitting them to be admitted based on their repetitive, procedural and routine nature and the regularity with which they are recorded as the solution to the difficulties which emerged in *Myers* of having to provide oral testimony informed by sufficient knowledge of the matters recorded therein.

4.59 Section 9 also has an effect on rules of procedure pertaining to disclosure in line with the Civil Procedure Rules 1988. Where evidence is to be received under section 9 without need for further proof, notice must be given to the opposing party of the intention to use such evidence.[29] This gives the opposing party notice and opportunity to inspect and challenge the document[30] and without this notice the evidence is not admissible.

4.60 Any higher foundational standards imposed in England for introducing electronic documentary materials have been dispensed with following the implementation of the *Civil Evidence Act 1995* which abolished the hurdles facing computer derived evidence and replaced them with a more relaxed scheme for admitting documentary evidence including what would otherwise be termed "documentary hearsay". The Act also restated the business document exception for civil proceedings and examples of documents which have formed part of the records of a business or public enterprise may now be admitted without further proof.

4.61 The provisions of the *Civil Evidence Act 1995* (section 8), incorporated in the criminal realm by section 133 onwards of the *Criminal Justice Act 2003* reaffirm that the emphasis has swung away from questions of admissibility in England and now rests on the means by which to apportion weight to the documentary evidence.

4.62 This shift in emphasis means that a document will not be admissible or will be counted as being of little probative value where its provenance and reliability cannot be established. This is particularly the case for real

---

29 Civil Rules of Procedure 33.6 (3).

30 Civil Rules of Procedure 33.6(8).

documentary evidence be it traditionally documentary or electronic in origin. In matters of documentary hearsay the issues concern documents which cannot be authenticated to the satisfaction of the court or in a manner approved by the court.

4.63 The business documents exemption represents an exception to the hearsay rule and is a means by which a documentary statement may be admitted in evidence without the need for accompanying oral testimony. The legislation regulating the admittance of these documents in criminal proceedings is section 117 of the *Criminal Justice Act 2003*. This provision is broadly similar to other jurisdictions and includes data records retained, created or received in the course of a business. The section also incorporates the judicial discretion to refuse to admit the document based on the judge's interpretation of the evidence advanced which tends to establish the reliability and provenance of the document or the circumstances surrounding the document or its transmission.

(b) Business Documents in Criminal Proceedings under the Criminal Justice Act 2003

4.64 In criminal proceedings many of the difficulties associated with proving documentary evidence were removed by section 27 of the English *Criminal Justice Act 1988* which carved out exceptions to the Hearsay Rule when it came to admitting documentary evidence coming from unavailable witnesses or business documents. These were then consolidated and incorporated in section 133 onwards of the *Criminal Justice Act 2003*.[31]

4.65 The 2003 Act represented a dramatic streamlining in the law regarding the admissibility of documentary hearsay evidence in criminal proceedings especially as concerned the authentication requirements for documentary evidence. This included the legal means by which to adduce evidence and identify the source and integrity of the document or any copy or derivative introduced in its place regardless of the number of removes from the original. Section 133 provides:

> "Where a statement in a document is admissible as evidence in criminal proceedings, the statement may be proved by producing either—
>
> (a) the document, or
>
> (b) (whether or not the document exists) a copy of the document or of the material part of it,
>
> authenticated in whatever way the court may approve."

---

[31] See paragraph 5.176, below.

4.66 Section 133 permits the use of copies in criminal proceedings irrespective of whether the original remains in existence. This reflects an increasingly inclusionary approach to the admission of documentary evidence by the English legislature extending the means of receiving a copy of the document so as to access the contents of the original. This also reflects the continuing distinction as between direct v hearsay documentary evidence and the internal dichotomy within hearsay evidence as between business and public records and other private documents with regard to presumptions of proof.

(3) The Exclusionary Rules Application in Australia

4.67 In Queensland, provision is made in the *Evidence Act 1977 (Qld)* through which documentary evidence can be admitted which might otherwise be classed as documentary hearsay. The 1977 Act includes, in this respect, certain public documents, transactions recorded in books of account, statements in documents pertaining to business records and trade documents and statements in documents produced by digital and electronic instruments. Given the duality of the Australian provisions there may be an overlap between these provisions for example where a book of account created by computer and there is the possibility of admitting it under both the provisions relating to books of account, as well as the provision that specifically deals with the admission of statements in documents produced by computers.

(a) An Australian Approach to Bankers' Books Exception at State Level

4.68 In Queensland, the scope of the traditional bankers' books provisions was expanded in section 83 of the *Evidence Act 1977* (Qld) to include commercial books of account of businesses and commercial entities aside from banks to include:

> "any document used in the ordinary course of any undertaking to record the financial transactions of the undertaking or to record anything acquired or otherwise dealt with by, produced in, held for or on behalf of, or taken or lost from the undertaking and any particulars relating to any such thing."

4.69 Section 84 of the *Evidence Act 1977* (Qld) provides that:

> (a) an entry in a book of account shall be evidence of the matters, transactions and accounts therein recorded; and
>
> (b) a copy of an entry in a book of account shall be evidence of the entry and of the matters transactions and accounts therein recorded.

4.70 Much as the term "document" is widely construed in section 3 of the *Evidence Act 1977* (Qld), so the term 'undertaking' is also widely defined as including:

> "public administration and any business, profession, occupation, calling, trade or undertaking whether engaged in or carried on—
>
> (a) by the Crown (in right of the State of Queensland or any other right), or by a statutory body, or by any other person; or
>
> (b) for profit or not; or
>
> (c) in Queensland or elsewhere."

4.71 The concept of an "undertaking" is clearly broader than simply a business operating for profit.

4.72 It should be noted that the books of account provisions apply to both criminal and civil proceedings. To fall within the definition of a "book of account" the document must satisfy the following criteria and be used in the ordinary course of that undertaking although this does not mean the document has to be used in a standardised format by all organisations of the type in question. The document must also record the financial transactions of the undertaking or:

> "anything acquired or otherwise dealt with by, produced in, held for or on behalf of, or taken or lost from the undertaking and any particulars relating to any such thing".

4.73 This seems to require that the document relate to the ongoing business of the undertaking in some way, although it is not limited to the formal financial records of an organisation.

4.74 The evidence covered by these provisions may be tendered without calling the person who made the record or the person who supplied the information. All that is required initially is that someone be available to give general identifying evidence that the record is indeed one of the undertaking and establishes that it was made in the usual and ordinary course of that undertaking. However, as the Australian Law Reform Commission noted in relation to provisions of this type:

> "If an attack is made on the accuracy of the record by the other party, the party tendering the record may be forced for tactical reasons to call persons involved in making the entries but it is not obliged to call them before the evidence is received".[32]

(i) Books of Account

4.75 The *Evidence Act 1977 (Qld)* lays down provisions for handling proof of transactions contained in books of account. Section 84 specifically provides

---

[32] The Receipt of Evidence by Queensland Courts: Electronic Records, Issues Paper WP No 52 Queensland Law Reform Commission, August 1998, p28.

that, in certain circumstances, an entry or a copy of an entry in a book of account is evidence of "the matters, transactions and accounts" recorded.

(ii) Statements in Documents

(I) Proceedings other than criminal proceedings

4.76 Section 92 of the *Evidence Act 1977 (Qld)*, is concerned with proceedings of a civil rather than criminal nature and lays down the criteria in which a statement contained in a document and which tends to establish a fact is admissible as evidence of that fact. Section 92(1) is divided for this purpose into two branches identifying the two distinct modes of evidence which may be admitted under each limb of section 92(1). These are statements which record first-hand information whether these are business records or not and those statements which convey information recorded throughout the ordinary course of an undertaking.

4.77 Both branches of section 92(1) ordinarily require the individual who made the statement or supplied the information contained therein to be called as a witness although provision is made in section 92(2) of the *Evidence Act 1977 (Qld)* for conditions which if satisfied mean that the requirement of witness testimony alluded to above may be dispensed with.

(II) Criminal Proceedings

4.78 Section 93 of the *Evidence Act 1977 (Qld)*, relates to evidence in criminal proceedings and established the conditions where a statement contained in a document and tending to establish a fact documented therein is admissible as evidence of that fact in defiance of the hearsay rule.

4.79 Although section 93 is similar to section 92 in many respects, it is narrower in its operation. Forbes suggests the following rationale for the relevant differences between the sections:

> "Section 93 uses language which, for the greater part, follows that of s92… Probably because of the higher standard of proof in criminal matters the gateway offered by s 93 is somewhat narrower than that provided by section 92."[33]

4.80 Section 93 does not contain an equivalent provision to the first limb of section 92(1). Rather, the operation of section 93 is confined to business records.

4.81 Forbes identifies another difference between sections 92 and 93:

---

[33] Forbes, JRS, *Evidence in Queensland*, 6th Ed, 2006, Lawbook Co.

> "Here [under s93] there is no question of tendering the document and calling the 'source' of the information…the statement is admissible only when the 'source' is absent for one of the reasons set out in s93(1)(b) …The grounds of permissible absence are narrower than in s92 and there is no question of producing both the document and the witness."

4.82 Both sections 92 and 93 deal with the admissibility of a statement contained in a document, rather than with the admissibility of the document itself.

(b) Admitting Business Records in Australia (Victoria)

4.83 Prior to the enactment of the *Evidence Act 1995*, like most jurisdictions Victoria had developed exceptions to the Hearsay Rule in order to admit "business" records in evidence. This exception was contained in section 55 of the *Evidence Act 1958* and extended the meaning of business to include public administration. To be admissible under this section the documents had to be created in the ordinary course of business (eg file notes, correspondence and briefings) and be based on information supplied by a person who had personal knowledge of it. In addition, and subject to some limiting exceptions, the person who supplied the information recorded in the document had to be called as a witness during the course of the proceedings.

4.84 The Australian admissibility of business records and the exemption from the full rigours of the rule against hearsay was updated and codified in section 69 (1) of the *Evidence Act 1995*.

4.85 A document may be a business record generated or maintained in the course of business dealings even where it is a draft document or a link in a chain produced "along the way" to completion of a final document which was confirmed by Barrett J in *Timms v Commonwealth Bank of Australia*.[34] With the advancement of the *Evidence Act 2008* in Victoria the *Evidence Act 1995* has been fully integrated into the law of evidence in Victoria. These provisions acknowledge the practicalities of conducting business through electronic means and integrate the business records exemption of the *Uniform Act 1995*.

4.86 A business document in this Act applies to a document which falls within the category of a document under the Act and exempts the document from the strict application of the hearsay rule if the document was made:

> "(a) by a person who had or might reasonably be supposed to have had personal knowledge of the asserted fact; or

---

[34] *Timms v Commonwealth Bank of Australia* [2003] NSWSC 576 at 17 and *NT Power Generation Pty Ltd v Power and Water Authority* [1999] FCA 1549, at 9.

(b) on the basis of information directly or indirectly supplied by a person who had or might reasonably be supposed to have had personal knowledge of the asserted fact."

(5) For the purposes of this section, a person is taken to have had personal knowledge of a fact if the person's knowledge of the fact was or might reasonably be supposed to have been based on what the person saw, heard or otherwise perceived (otherwise than a previous representation made by a person about the fact)."[35]

(4) Authenticating Commercial and Business Records in Australia (Victoria)

4.87 In acknowledgement of the possibilities represented by e-transacting, the *Electronic Transactions Act (Victoria) 2000* was introduced in order to encourage electronic means of doing business by removing real or perceived legal barriers.

4.88 Much like the Irish legislation the Act does this by statutorily expunging any presumption or suggestion that a transaction is somehow less valid because it is conducted electronically. It nurtures public and business confidence in the use of electronic transactions and lays out a framework for recognising the legal validity of e-transactions as well as allowing the "recording and retention of information in electronic form."[36]

4.89 This final stipulation facilitates entities who wish to transform their organisation into a paperless office by scanning and retaining previously paper based data into an electronic form.

4.90 The *Victorian Electronic (Transactions) Act 2000* does not give carte blanche to a business to scan documents and dispose of the original. Instead it imposes limitations to prevent the frustration of the hearsay rule and as a means to mitigate potential concerns about electronic records. The process is examined with an eye to the longevity of the document whereby the scan must be produced through a system capable of maintaining the integrity of the record over time. This recognises the role of the process and resulting copies which can only be as good as the process which produces them and which should include authentication and quality assurance.

4.91 Secondly, the format of the newly digitalised document is examined. The Act imposes a format on an organisation wishing to avail of the provision. The document must be presented in such a way that makes it "readily available

---

35 *Evidence Act 1995*, section 69 (2) and (3) and incorporated within the *Evidence Act 2008* of Victoria in section 69

36 *Electronic Transactions Act* (*Victoria*), 2000 Sections 11 and 12.

for subsequent reference" meaning that the electronic file must not require the courts or the user to search out obsolete or rare technology in order to read the file. This is a pragmatic provision to increase access to electronic or automated documents and facilitate their production in evidence.

4.92 Other pieces of legislation such as the *Crimes (Document Destruction) Act 2006* in Victoria combine with the provisions of the *Evidence Act* to provide a very comprehensive framework by which to adjudicate on the admissibility of documentary evidence. Through section 51 the *Evidence Act 2008* removes the impediment represented by the Best Evidence Rule so as to permit copies and extracts to be admitted in evidence. This also acknowledges the practicalities of conducting business through electronic means and with the *Crimes (Document Destruction) Act 2006* permits the digitisation of hard copy documents and the destruction of the original when undertaken as part of a records management system. This prevents against duplication of documentation and is both a cost and labour saving provision. However, perhaps keen to ensure that this cannot be used as a legislative carte blanche to destroy and erase sensitive and potentially damaging documents, in some circumstances the original must be preserved even where this has been digitised and the legislation has also introduced offences for the destruction of documents which could reasonably be foreseen as necessary for any future litigation.[37]

(i) Admissibility of Liquidators Reports as Business Documents

4.93 The question of whether liquidators' reports are admissible as the business documents of the firm under investigation or whether they are the products of the liquidators' business and therefore not classed as business records has also been discussed in Australia. An analogy was drawn between these reports and a report commissioned by a company in the course of conducting an investigation for which it was paid. In *RW Miller & Co Pty Ltd v Krupp (Australia) Pty Ltd*[38] Giles J held that for the purposes of Part IIC of the *Evidence Act 1898 (NSW),* such a report was not a business record as it did not arise during the ordinary course of the day to day activities of the firm.

4.94 A counter argument was made in *ASIC v Rich*[39] that the copies of a liquidator's report retained by the liquidator did qualify as a business record. This was based on a similar situation in the US where liquidators' reports and the reports made by a company to the United States Securities and Exchange

---

37 *Crimes Act 1958 section 254.*

38 (1991) 32 NSWLR 152.

39 [2005] NSWSC 417.

Commission had been held to be business records in *Ritz Hotel Ltd v Charles of the Ritz Ltd (Nos 13, 18 and 19).*[40]

(5) The Production of Documents in Evidence under the Bankers' Books Evidence Acts

4.95 The 1879 Act, as amended, is phrased so as to compel the production of documentary evidence from a financial institution on production of an order of the court having been made. Should a bank refuse to so furnish a verified copy of an account in accordance with section 3 of the 1879 Act, case law suggests that they may be ordered to produce the books containing the account in question at the trial of the action as occurred in *Coleman v Coleman.*[41] The bank in question (Ulster and National Bank) refused to produce such verified copies without an order of the Court. O'Brien J noted that although the 1879 Act permitted that an order be sought, it was "quite irregular" for the bank to refuse to give a copy until receipt of notice of an order of the Court.

4.96 The interpretation of the *Bankers' Books Evidence Acts* as a statutory erosion of the duty of banking secrecy pre-dates the decision in the English case *Tournier* v *National Provincial and Union Bank of England* where Bankes LJ described the common law duty of secrecy as disclosure by compulsion of law.[42] In 2007, *Tournier* was accepted as correctly stating Irish law.[43]

4.97 The first and most wide-ranging of Bankes LJ's exceptions referred to disclosure by compulsion of law. In Ireland the Oireachtas has, on various occasions, including in the *Criminal Justice Act 1994*, considered that public policy justified the introduction of a statutory provision which required bankers to disclose their customers' financial affairs. In this section, the Commission turns to consider the most important statutory provisions and, where applicable, the way in which they have been treated by the courts.

4.98 *Tournier v National Prudential and Union Bank of England* arose from proceedings involving the plaintiff customer of the defendant bank who had gotten into financial difficulty and entered an agreement with the defendant bank to pay back the money owed in stages. When the plaintiff's repayment was late, the bank manager telephoned his employers and revealed the plaintiff's financial difficulties and suggested the possibility that he was engaged

---

40 (1988) 14 NSWLR 116 at 122. This followed a finding that the reports were made on foot of a statutory provision which required such records to be made as a necessary incident of the carrying on of the business.

41 (1898) 32 ILTR 66.

42 *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461.

43 *Walsh v National Irish Bank Ltd* [2007] IEHC 325, [2008] 1 ILRM 56, para 17.

in gambling. As a result of the conversation, the plaintiff lost his job. The Court of Appeal held that the bank was in breach of its duty of confidentiality and took the opportunity to explore in detail the ambit of this duty. This case establishes the proposition that it is an implied term of any contract between a banker and its customer that the bank will not divulge to third parties, without express or implied consent, the account details, the history of transactions or other information acquired by the bank during its relationship with the customer. It has been noted that this case has been applied in numerous other decisions in England[44] and is regarded as correctly reflecting the law in Ireland, where it has been accepted that a duty of confidentiality exists although underpinned by public interest considerations such as those which were recognised by the Supreme Court in *National Irish Bank Ltd v Radio Telefís Éireann.*[45]

4.99 Sections 3 to 6 of the *Bankers' Books Evidence Act 1879*, as amended, enable attested copies of entries in a banker's books to be admitted as evidence speaking to the contents of these books in accordance with an order made on application to the courts. This serves to admit evidence which would otherwise engage the rule against hearsay. Thus while banks owe an obligation of confidentiality to their clients, this duty is qualified by the demand of an over-riding public interest where this is better served by the disclosure of the documents. Sections 3 to 6 of the 1879 Act from this perspective enable such evidence to be admitted without the production of the physical original books and testimony of a banking official "when the public duty supersedes the duty of the agent to the principal."[46]

4.100 Section 7 of the 1879 Act provides that, on the application of any party to legal proceedings, the court has the jurisdiction to order that a party be given liberty to inspect and take copies of any entries in the bankers' books before trial whether the books in question relate to the account of a party to the litigation or to that of a third party. Section 7A of the 1879 Act, inserted by section 131 of the *Central Bank Act 1989*, provides that if, on an application made by a Garda Superintendent, a court or a judge is satisfied that there are reasonable grounds for believing (a) that an indictable offence has been committed; and (b) that there is material in the possession of a bank specified in the application which is likely to be of substantial value (whether by itself or together with other material) to the investigation of the offence, then a court or

---

44 *Re State of Norway's Application (Nos. 1 and 2)* [1989] 1 All ER 745*; Lipkin Gorman v Karpnale Ltd* [1992] 4 All ER 409 and *Barclay's Bank v Taylor* [1989] 3 All ER 563.

45 [1998] 2 IR 465 at 494.

46 *Waterhouse v Barker* [1924] 2 KB 759; [1924] All ER Rep 777, CA, at pp. 771, 772 and p 783, per Atkin, LJ.

judge may make an order that the applicant or another member of the Garda Síochána designated by him be at liberty to inspect and take copies of any entries in a banker's book for the purposes of investigation of the offence.

(6) When is a Document (Particularly an Electronic Document) "Kept" by a Bank?

4.101 The *Bankers' Books Evidence Acts*, as amended, are clearly capable of adapting (along with common law principles) to ensure the admission in evidence of documentary data held by financial institutions. The principle of the common law as continuing to apply even in "today's world of highspeed technology and communication"[47] has already been acknowledged. This takes account of the shift from physical retention to virtual retention of documentary evidence in the banking sphere. Since hardcopy bankers' books and manual hand-executed ledger entries have long been phased out in favour of computerised mass-storage systems, it may be necessary to address the interpretation of how documentary information is "kept".

4.102 The extent to which the operational jurisdiction of a bank account in relation to computerised documents extends arose in the English case *Libyan Arab Foreign Bank v Bankers Trust Co.*[48] where the Court addressed the issue of determining admissibility of evidence of bank accounts held on a computer. On the jurisdictional matter the Court noted:

> "it may not be strictly accurate to speak of the branch where the account is kept. Banks no longer have books in which they write entries; they have terminals by which they give instructions; and the computer itself with its magnetic tape, floppy disc or some other device may be physically located elsewhere. Nevertheless it should not be difficult to decide where an account is kept for this purpose, and it is not in the present case."[49]

4.103 He held that while made on instruction from New York, the actual entries in the London account were made in London and were thus legally "kept" and retained there. Thus they were discoverable as documentary evidence to the English courts.[50]

---

47 *Walsh v National Irish Bank Ltd* [2007] IEHC 325, [2008] 1 ILRM 56, para 28.

48 *Libyan Arab Foreign Bank v Bankers Trust Co.* [1989] QB 728.

49 *Ibid,* at 746.

50 While the above is illustrative of the situation at common law as regards the extra-territorial operation of an order effectively permitting the gathering of documentary evidence from a financial institution statute law had also directly intervened in this

(7) The Extent of a "Record" under the Bankers' Books Evidence Acts

4.104 It must be born in mind that though an order for inspection can be made *ex parte,* the order and the resulting documentary evidence remains subject to the same general criteria as discovery orders. It is not to be viewed as a "fishing expedition". The section creates no new power of discovery[51] but rather it creates a legal environment through which a third party's accounts may be treated as the accounts of a party to the litigation.[52]

4.105 To this end the inspection of a third party's account will only be ordered to the extent that the documentary information sought is, in form or substance, the account of a party to the litigation.[53] "Fishing expeditions"[54] are not permitted under section 7 of the 1879 Act, and nor are they acceptable under the ordinary rules of discovery. An order for inspection may be refused where one party attempts to gain access to bank records in circumstances where the other party has disclosed all the relevant entries in his pass book and has submitted an affidavit to the extent that all other entries in the books of the bank are irrelevant.[55]

4.106 The power to order inspection of a third party's accounts is available but discretionary as discussed in *Emmott v Star Newspaper Co.*[56] and so is exercised sparingly.[57] In *Staunton v Counihan*[58] Dixon J stated that the

---

area. In Ireland, the *Contractual Obligations (Applicable Law) Act 1991* gave the force of domestic law to the 1980 Rome Convention on Applicable Law.

51 *Arnott v Hayes* (1887), 36 Ch D 731, CA, at p. 737, per Cotton, LJ.

52 *Howard v Beall* (1889), 23 QBD 1.

53 *Howard v Beall* (1889), 23 QBD 1 and *Pollock v Garle,* [1898] 1 Ch 1, CA.

54 "Fishing" is described by Kerr LJ in *In re Jahre (Anders)* [1986] Lloyd Rep 496, at 515 as an investigation which arises where "what is sought is not evidence as such, but information which may lead to a line of enquiry which would disclose evidence. It is the search for material in the hope of being able to raise allegations of fact, as opposed to the elicitation of evidence to support allegations of fact, which have been raised bona fide with adequate particularisation." Also see Binchy, *Irish Conflicts of Law,* Butterworths, 1988, p 636.

55 See *Parnell v Wood* [1892] P 137.

56 (1892), 62 LJQB 77.

57 *South Staffordshire Tramways Co. v Ebbsmith,* [1895] 2 QB 669, CA, at p 674, per Lord Esher, MR.

58 (1958) 92 ILTR 32.

jurisdiction to make an order under section 7 of the 1879 Act must be exercised cautiously even where the account holder is a party to the action. In instances where the account is of a third party not joined to the action even more caution is required. Here it was not enough for the applicant to show that it may have proved useful to see the entries. He was required to show that the entries are essential to his action and would be admissible. In a similar vein Andrews J stated in *L'Aime v Wilson* that:

> "it would be monstrous to suppose that it was the intention of the Legislature that the Court might enable any party to legal proceedings to inspect and take copies of any entries in the banking accounts of any other people".[59]

4.107 Section 7 of the 1879 Act is therefore neither arbitrary and nor does it overstep its stated purpose. The 1879 Act, as amended, does not permit a party to embark upon a wholesale search of bank accounts and in the English case *Williams v Summerfield*[60] Lord Widgery CJ noted in support of this proposition that:

> "The courts have set their face against section 7 being used on a kind of searching enquiry or fishing expedition beyond the usual rules of discovery."

4.108 This proposition has also been judicially stressed in Ireland in *Staunton v Counihan*[61] as it could not be shown that the entries in the account were sufficiently material to an issue in the action so as to be clearly and necessarily admissible in evidence against the defendant.

4.109 The bankers' book exemption from the strict application of the exclusionary rules regulated by the *Bankers' Books Evidence Act 1879* and as amended has remained a live issue. They are of particular relevance in proceedings arising from attempts to adduce evidence from abroad eg as from financial institutions in fraud cases and particularly where any potential witnesses are not compellable as witnesses.

4.110 The bankers' books exception to the exclusionary rules of evidence which permit secondary evidence of banking and business records to be introduced in evidence has been litigated successfully in regard to the international money laundering dimension of both the parent Act and subsequent legislation which has been subject to constitutional challenge.

---

59 [1907] 2 IR 130.

60 [1972] 2 QB 512.

61 (1958) 92 ILTR 32.

4.111 The 2005 case of *Volkering and Others v District Judge Haughton and Another,*[62] is a good example of a modern Irish application of the Best Evidence Rule and one of the many exceptions adapted out of necessity in relation to it. It discusses previous case law and concludes that this exception ought to be interpreted broadly. Among other issues the case discussed and decided the boundaries of what constitutes a "record" for the purposes of gathering documentary evidence within the perimeters of the legislation.

4.112 The applicants claimed relief by way of judicial review in relation to two orders made by the respondent under section 51 of the *Criminal Justice Act 1994*.[63] That section, in conjunction with the Second Schedule to the Act, established a procedure for the taking of evidence within the State for use in a criminal prosecution in another jurisdiction and which permitted certain documents relating to a particular bank account held with the Bank of Ireland to be admitted in evidence. It was stated that each of those documents constituted "an entry in a banker's book" such as would render them admissible in evidence under the exception to the Best Evidence Rule under sections 4 and 5 of the *Banker's Books Evidence Act 1879* as amended.

4.113 The applicants argued that the documents did not fall within the terms of the 1879 Act so as to exclude them from the statutory exception to the rule against hearsay or the Best Evidence Rule laid out in section 3 of the 1879 Act. Opposing counsel raised the dicta in *JB, O'C v PCD*[64] where Murphy J had

---

62 [2005] IEHC 240.

63 The *Criminal Justice Act 1994* created an offence of money laundering and made provision for international co-operation in respect of certain criminal law enforcement procedures. The Act implements Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering. Part VII updates existing criminal law procedure powers facilitating international mutual assistance in criminal investigations or prosecutions. The Act also enables the State to ratify the Council of Europe Convention on Mutual Assistance in Criminal Matters (1959), the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (1990) and the Vienna Drugs Convention (1988).

Section 51 is a section under the general heading of International Co-operation and accommodates the taking of evidence in the State for use outside the State. The Second Schedule to the Act, which deals with the taking of evidence for use of outside State, has a supplementary provision ratifying that the *Bankers' Books Evidence Act, 1879*, "applies to the proceedings as it applies to other proceedings before a court."

64 [1985] IR 265 at 273-4, which considered *R. v Jones* [1978] 1 WLR 195 (letters not being records); *Barker v Wilson* [1980] 1 WLR 884.

referred to the amendment of the 1879 Act by the 1959 Act by the inclusion of the word "record" and it was submitted that if this definition of "an entry in a banker's book" was to apply to the documents under consideration then a conclusion would be reached as in both *JB, O'C v PCD* and *Williams v Williams*[65] to the effect that the documents would not fall within the terms of the *Bankers' Books Evidence Act 1879.*

4.114 As noted by the court in *JB, O'C v PCD* the question of whether letters contained in a bank's correspondence file could be construed as "bankers' books" was dealt with by the English Court of Appeal in the 1983 case of *R v Dadson*.[66] The letters at issue in that case were two copy letters from the bank concerned to the appellant. Each letter related to a separate cheque drawn by the appellant on his account, and each requested that the cheque concerned should be presented only after sufficient funds had been lodged to the account. The conclusion reached was that:

> "whilst the *Bankers' Books Evidence Act* enables evidence to be admissible in a court by the production of copies, rather than originals, it does so provided only that the book, one of the types referred to in that section, is one of the ordinary books of record of the bank, and the entry was made in the ordinary course of business. It is therefore manifest that those letters could not be brought within the clearly expressed language of that Act. They are not "bankers' books" and in the judgment of this Court they should not have been admitted."

4.115 However the Irish court in *Volkering* determined on appeal that under the provisions of section 51 of the 1994 Act, the function of the judge was to receive and not to prove the evidence and so no restrictive definition of bankers' books could detract from the discretion enjoyed by a nominated district judge to receive documentary evidence as he deemed appropriate in the circumstances.

(8) Documentary Evidence of Bank Records Produced by Electronic Means in Australia

4.116 Section 95 of the *Evidence Act 1977 (Qld)* sets out the circumstances in which a statement contained in a document produced by a computer and tending to establish a fact is evidence of that fact can be admitted in evidence.

4.117 The admission of a document and the position of the opposing party to show that the computer was prone to malfunction, or that there is some other

---

65 [1998] 1 QB 161.

66 *R v Dadson* [1983] 77 Cr App R 91.

reason to question the reliability of the record is a matter that the court may take into account when ultimately deciding what weight to give to the document.

4.118 The implication of the enactment of these special provisions and allowances relating to bankers' books demonstrates that legislatures are predominantly satisfied that such records including computer-derived documents, are likely to be kept accurately, more accurately it seems than mere computer output where for example that output has not itself been used in the course of carrying on a banking business.

4.119 However, these provisions do not generally make a copy of a banking record conclusive evidence of the matters to which it relates and, where the reliability of the record is convincingly challenged, it will be for the court to decide on the whole of the evidence and whether it should act on the documents that are put before it.

(a) Scope of the Books of Account Provisions regarding Computerised Documents and Electronic Derivatives

4.120 While the Queensland legislation does not specifically provide for the admission or otherwise of computerised books of account there is nothing to suggest that their operation does not extend to books of account that comprise digitally generated documents.

4.121 In *ANZ Banking Group Ltd v Griffiths*[67] the Supreme Court of South Australia held that a copy of a microfiche was a copy of a banking record within the meaning of section 46 of the *Evidence Act 1929* (SA) and was admissible under section 47 of that Act. The documents in question consisted of photocopies of duplicate bank statements relating to an account of the respondent.

4.122 The matter arose as to whether the documents produced by the computer from data relating to banking transactions recorded and stored by a bank upon the computer were copies of a banking record within the meaning of section 46 of the *South Australian Evidence Act 1929* and if so whether any such documents were admissible pursuant to section 47(1) of the South Australian Act.

4.123 The data from which those statements were compiled was stored in the bank's computer and had at some stage been printed out for convenience on microfiche.

4.124 At first instance it was held that section 46 of the *South Australian Act* did not include computer records because there was no reference to computers in that section, and it would therefore artificially extend the definition of 'copy' to

---

67 (1988) 49 SASR 385.

infer that sections 46 and 47 encompassed computers. Millhouse J on appeal ruled that the definition of "copy" in the *South Australian Act* did extend to include a copy of a record made by a computer.[68]

4.125 On appeal in *Griffiths v Australia and New Zealand Banking Group Limited*,[69] the Supreme Court of South Australia confirmed this latter conclusion and also held that the copy of the microfiche record of the computer record was a "copy" for the purposes of the South Australian provisions. This came about because the microfiche had been generated by the bank, for the use of the bank in the ordinary course of its business and thereby it fell squarely within the meaning of a banking record so that a copy of it was a copy of a banking record for the purposes of section 46.

> "Whatever may be the status under these sections of the computer data itself...(i)f the print-out remains in the possession or control of the bank, and is used as an accounting or other record by the bank in the course of carrying on its banking business, it will become a 'banking record' in its own right. That, on the uncontradicted documentary and oral evidence presented by the respondent, was the position with respect to the microfiche records in this case."[70]

4.126 The Queensland Law Reform Commission did not believe that this decision could stand as authority for the proposition that any computer printout of a business record, or copy of such a printout, would be admissible under s 46 as proof of the matters recorded in it. It was important in *Griffiths* that the microfiche from which the copy had been made was held to constitute a banking record in and of itself. The court did not go further and determine whether the data recorded in the computer itself constituted a 'banking record', or whether a printout generated for the purposes of the litigation would have been admissible under the banking records provision.[71]

4.127 However, in *Markovina v The Queen*,[72] the Supreme Court of Western Australia examined the admissibility as evidence of electronic diaries of a person charged with drug-related offences. It adopted a pragmatic

---

68 (1988) 49 SASR 385 at 388.

69 (1990) 53 SASR 256.

70 *Ibid,* Cox J at 262.

71 Receipt of Evidence by Queensland Court: Electronic Records Issues Paper, WP No. 52, 1998, p 46.

72 (1996) 16 WAR 354.

approach and held that the "diaries were a record of business dealings and could be looked at in the same way as entries in books of account."[73]

(9) The Evolution of and Amendments to the Bankers' Books Evidence Act and Counter money Laundering Provisions- Still Relevant Today?

(a) The Bankers' Books Evidence Act 1879 as Amended

4.128 The *Bankers' Books Evidence Act 1879* has been amended in consequence to the changing financial and banking environment. *The Bankers' Books Evidence (Amendment) Act 1959* was initiated to remedy any lacunae which had arisen since the enactment of the 1879 Act and to take account of the changing perception of a "bank" to accommodate other financial and credit institutions.[74]

4.129 While the *Bankers' Books Evidence Acts* might appear to represent archaic provisions designed for the regulation of physical books and documents, as clear from the above case law, they have not stayed rigid and static. Rather than ignoring the modern means of technologies used in the banking sectors, legislation has adapted and developed to stay in line with these emerging technologies. Whereas the English courts have accepted an extended analogous meaning of "books" without the need for any legislative amendment,[75] section 9 of the 1879 Act, as amended by section 2 of the *Bankers' Books (Amendment) Act 1959*, provides that bankers' books:

> "(a) include any records used in the ordinary business of a bank, or used in the transfer department of a bank acting as registrar of securities, whether comprised in bound volumes, loose-leaf ledger sheets, pages, folios or cards, and:
>
> (b) cover documents in manuscript, documents which are typed, printed, stencilled or created by any other mechanical or partly mechanical process in use from time to time and documents which are produced by any photographic or photostatic process."

4.130 As already noted, section 131 of the *Central Bank Act 1989* further extended the definition to include computer records. Section 131 of the 1989

---

73 (1996) 16 WAR 354, Malcom CJ at 380.

74 This is in line with section 9 or to comply with section 11 of the *Revenue Friendly Societies and National Debt Act 1882* which section 3 of the 1959 Act went on to repeal in favour of inserting an updated definition of a "bank" in section 9 and a "bankers' book" in section 9 (2)(a) and (b).

75 *Barker v Wilson* [1980] 1 WLR 884.

Act also inserted section 7A into the 1879 Act, which extended the category of parties entitled to make an application under the Act to include members of the Gardaí investigating a criminal offence.

4.131 These legislative extensions have not been as thorough as envisaged as was discovered in the 1985 case of *JB, O'C v PCD*[76] which concerned section 18 of the *Finance Act 1983*. However the limitations of the definition of bankers' books in the *Bankers' Books Evidence (Amendment) Act 1959* were also of relevance. Murphy J considered that the word "books" in this context did not extend to files or correspondence or any other documents which did not "constitute a book within the extended meaning of that word".[77]

4.132 Other legislative provisions with the power to impinge directly on the disclosure and the gathering of evidence held by a party other than one of the litigants include section 18 of the *Finance Act 1983* which allows an officer of the Revenue Commissioners to make an application to the High Court requiring the financial institution to furnish the Revenue Commissioners with "full particulars of all accounts maintained by" the impugned party within the ten years prior to the application and with such other information "as may be specified".

4.133 As previously stated the Commission would not support a different system to regulate electronic as opposed to paper-based documentary evidence. To that end the Commission has recommended a more far-reaching and elastic interpretation of the definition of a document in an effort to encourage the admissibility of electronically generated evidence.

(10) Determining the Authenticity and Integrity of a Business Record

4.134 Where a document is adduced under and has complied with the provisions of *Bankers' Books Evidence Acts* there remain the challenges of establishing its authenticity, integrity and the confidentiality with which it has been maintained. The prospect that information held by a financial institution in a computer memory being adduced in evidence but having been altered before or after being reproduced in legible form and adduced before the court is a possibility. The Commission is of the opinion that no prescriptive legislative provisions should be enacted which would require a litigant to show the workings of its computer system. Were the situation illustrated to arise it could be challenged by tendering the customer's copies of deposit slips and cheque receipts and the authenticity and integrity of the document as challenged would then go to weight. In this way the parties themselves are the vetting mechanism

---

76 [1985] IR 265.

77 At 274. This is in line with the English cases in the area. See Ellinger and Lomnicka *Modern Banking Law* (2nd ed, 1994).

by which to ensure the integrity and veracity of the documentary evidence adduced by the other party.

D Modern Applications of the Bankers' Books Evidence Act- A Tool Against Fraud

(1) Developments at European Level

4.135 The EU has recognised the need to regulate the international transfer of funds in order to combat money laundering. This led to the approval of the First Money Laundering Directive in 1991.[78] Ireland implemented the 1991 Directive in the *Criminal Justice Act 1994.* Part IV (sections 31–32) and Part VIII (sections 57–60) of the 1994 Act introduced the offence of money laundering and placed certain detection, reporting and internal procedural obligations on financial institutions so to ensure against their facilities being used for the purposes of money laundering.

4.136 This was considered in *JB, O'C v PCD*[79] holding that legislation which encroached upon the duties traditionally owed to a customer would be interpreted narrowly.

(2) Gaining Access to Business Records and the Director of Corporate Enforcement

4.137 Section 10(2) of the *Companies Act* 1990 has important implications for banks because it conferred broad powers of inquiry on company inspectors. It confers powers of investigation and compels disclosure by a corporate entity who must produce to inspectors any books or documents relating to the company or other body corporate or to attend before them to offer assistance with the investigation.

4.138 The *Companies (Amendment) Act 2009* grants additional powers to the Director of Corporate Enforcement in relation to the powers of search and seizure but also as regards the access to documents held by corporate entities and the responsibility to disclose ass such documentation. This builds upon and also updates the bankers' books provisions and grants considerable access to business books even where these are in the possession of third parties. Documentation relevant to litigation cannot therefore be shunted around a group of companies to prevent its disclosure. This extends to the primary documents themselves but also to copies of these records and documents

---

78 EC Council Directive 91/308 on the prevention of the use of the financial system for the purpose of money laundering [1991] OJL 66/77.

79 [1985] IR 265.

under section 4(1)(a). This then has considerable implications for the disclosure of documents sought by the Director of Corporate Enforcement.

4.139 The 2009 Act also provides for the removal from premises for inspection of electronically held evidence which could form part of a computer system. Section 20 of the *Companies Act 1990*, as amended by section 5 of the 2009 Act, provides that the Director may seize records which may not form part of a "book, document or other thing" (so called seizeable information) but which is relevant and comprised in something else which he has no power or remit to seize. This could certainly permit electronic documents to be discovered or seized where held within a computer or electronic storage system.

4.140 In regard to the register of loans and charges maintained by corporate bodies and detailing the loan activities of a back, section 9 of the 1990 Act states that, where sought by the Director of Corporate Enforcement, a company shall produce the register maintained by it and must also permit copies to be made and removed for examination.

4.141 In *Chestvale Properties v Glackin*[80] it was suggested that the provision was an unacceptable trammeling on the contractual right of the customer to enjoy confidentiality with his banker. However Murphy J held this to be a limited invasion and one which was justifiable in the circumstances.[81] In *Chestvale Properties v Glackin (No. 2),*[82] the obligations this placed on the bank were considered and were interpreted as compelling a bank to "produce all books and records in their possession which may be of assistance to the inspector in connection with this investigation into the membership of the companies."

4.142 The necessity of admitting bank records has been widely embraced. In South Africa the governing provisions remain differentiated along the civil/criminal divide. Both are facilitated by extending existing legislation to include newer technologies. For records required for litigation in the criminal law the relevant provision is section 236 of the *Criminal Proceedings Act 1977* on the proof of entries in accounting records and documentation of banks which exempts bankers' books and records from the operation of the Hearsay Rule. The section has had its phraseology updated to include in the definition of document as a "recording or transcribed computer printout produced by any

---

80 [1993] 3 IR 35.

81 *Ibid*, at 45–46.

82 High Court, 10 March 1992.

mechanical or electronic device and any device by means of which information is recorded or stored."[83]

4.143 South Africa had not attempted to introduce a piece of legislation to address the admissibility of banking records and is therefore a good example of how the two legislative regimes can coexist. In civil proceedings banking records can be made available as *prima facie* evidence of their contents under part 5 (sections 27-32) of the *Civil Proceedings Evidence Act 1965*. The continuing use of this law was evident in the 2006 case *Nedbank Ltd v Mashiya and Another.*[84]

(3) The Foreign Dimension to the Operation of the Bankers' Books Evidence Act 1879

4.144 Owing to the increasing volume of international commercial transactions, commentators have highlighted the ever growing importance of the foreign operation of the 1879 Act.[85] The issues in this context centre on whether an order of an Irish court has extra-territorial effect and also whether an Irish bank must correspondingly comply with a foreign court's order to disclose information.

(a) Extra-territorial Effect of the Legislation

4.145 The *Central Bank Act 1989* also influences the manner in which cross-jurisdictional documentary evidence of business records held by a banking institution may be tendered in evidence. Section 16(2)(e) of the *Central Bank Act 1989* regulates the disclosure of banking records to a foreign jurisdiction to aid an investigation.

4.146 This builds on section 18(2) of the *Central Bank Act 1989* which states that the information may be transferred and kept "otherwise than in legible form so long as the recording is capable of being reproduced in a legible form". This solves any issues surrounding the admissibility of derivative evidence because it allows for the production of a copy reproduced, essentially generated for perhaps the first time in tangible tactile form. This copy is deemed sufficient to satisfy any evidential requirements. This lifts any burden which would otherwise be on a financial institution to "keep" documents relating to the operation of the bank in physical form. Permitting electronic storage means that

---

83 Section 236 (5).

84 2006 (4) SA 422 (T) at 427 para 26.

85 Donnelly "*The Erosion of the Bankers' Duty of Secrecy*", (1996) 3(9) CLP 226.

the legislation lends itself towards commercial realism and the balance of convenience for the institution in question.[86]

4.147 As already noted, the *Central Bank Act 1989* made several amendments to the *Bankers' Books Evidence Act 1879,* including making allowances for the primarily electronic nature of many banking systems for recording and holding documents and account records. Section 5 of the 1879 Act was amended so that a copy of an account will not be deemed to be sufficient evidence unless it is "further proved" that it has been effectively reproduced from non-legible to legible form[87] and to this end that it has been compared to a copy so produced and found to be correct[88] or has been compared with an original where available.[89] This can be satisfied on production of either oral testimony or an affidavit submitted to the court.[90]

4.148 It must be noted that the 1989 Act also amended section 6 of the 1879 Act by the removal of the words "to which the bank is not a party," opening up the possible litigation to which the bank may be joined.

4.149 Concurrent and supplemental to the *Bankers' Books Evidence Acts* is section 908 of the *Taxes Consolidation Act 1997* as substituted by section 207 (1) of the *Finance Act 1999*. This permits an application to the High Court by a litigant seeking an order to direct the disclosure of documentary account evidence by a financial institution. It also allows an authorised officer of the Revenue Commissioners to investigate an institution's account documents where that officer is of the opinion that the existence of these accounts has not been disclosed to the Revenue Commissioners or that the figures maintained are false or misleading.

4.150 The question of the extra-territorial effect of an order centres on whether an order of the Irish High Court suffices where the institution is located outside the State. This arose in *Chemical Bank v McCormack*[91] where Carroll J rejected the argument that the 1879 Act had an extraterritorial effect and refused to allow documentary evidence to be taken form a New York branch. This was among other things in the interests of the comity of the courts.

---

86 Section 18 (3).

87 Section 5 (1) (a).

88 Section 5 (1) (b) (i).

89 Section 5 (1) (c).

90 Section 5 (2).

91 [1983] ILRM 350.

4.151 The issue was also addressed in *Walsh v National Irish Bank Ltd*.[92] This case concerned the attempt to retrieve documentary evidence from a branch of the National Irish Bank located in the Isle of Man. While the objections were jurisdictionally based, the order was also addressed to an Irish banking entity. The Offshore Assets Group had been set up within the Investigations and Prosecution Division of the Revenue Commissioners to identify and deal with Irish residents who might have sought to evade their tax liability by the use of offshore accounts. The respondent was a licensed Irish bank which opened a branch in the Isle of Man providing deposit facilities and which continued to do until it surrendered its banking licence to the Isle of Man authorities in 1992.

4.152 The applicant officer in the Offshore Assets Group brought an application to the High Court pursuant to section 908 of the *Taxes Consolidation Act 1997*[93] seeking an order directing the respondent to furnish documentary data including a schedule of the names of deposit account holders with an address in the State. The respondent objected and countered that the court had no jurisdiction to make such an order as it did not relate to a branch which was resident in this jurisdiction.

4.153 The applicant argued that, as the order sought was directed towards an Irish entity, which was capable of performing its terms within the territorial jurisdiction of the State and related to the accounts of Irish citizens, it should be granted access to the information requested under the 1997 Act. The respondent countered that it owed a duty of confidentiality to its customers and conforming to the order would mean breaching this duty. As to the cross-jurisdictional nature of the order, the respondent also submitted that the governing law of contract between a banker and its customers was that of the jurisdiction in which the branch was located rather than where transactions were capable of being exercised, and that any application would have to be taken in the Manx courts.

4.154 McKechnie J refused to make the order sought and held that it had been long established that the contractual relationship between a banker and its customer is predicated on an obligation of confidentiality and that such information is to be maintained by the bank alone, except where the express or implied consent of the customer has been obtained. This duty extended beyond the term of the contract and the respondent remained under a duty of confidentiality to its former account holders in the Isle of Man.

4.155 It was acknowledged that this duty was not absolute and is subject to qualification where disclosure was under compulsion of law, where there was a

---

92 [2007] IEHC 325, [2008] 1 ILRM 56.

93 As substituted by s 207(1) of the *Finance Act 1999*.

duty to the public to disclose, where the interests of the bank required disclosure or where the express or implied consent of the customer had been obtained.[94]

4.156 McKechnie J held that a contractual banking arrangement which related to an account was governed by the jurisdiction in which that account was held despite the possibility that the parent company of the branch in which the account was kept was in a different jurisdiction.

4.157 It was also noted that, without the clearly expressed intention of the Oireactas to the contrary, there was no perceivable intention expressed in section 908 of the 1997 Act and it must be presumed that the Oireachtas did not intend that the 1997 Act would operate beyond the territorial limits of the State. This proposition was bolstered by reference to the decision of Carroll J in *Chemical Bank v McCormack.*[95]

4.158 While it was decided not to grant the order in this instance, the discretion of the court to so order was preserved. This limitation on the power of the Irish courts to enforce compliance with its orders extra-territorially avoids any resulting conflict which could arise if the foreign jurisdiction had different rules to the Irish ones in relation to secrecy.

(4) Need to retain Bankers' Books exemption to the exclusionary rules of evidence.

4.159 It has been judicially noted that the *Bankers' Books Evidence Act* is a "facility to prove a banker's account by way of sworn evidence of the banker."[96] Business records and bankers' books exemptions were introduced as an acknowledgement of the mundane nautre of the classes of records with which they are concerned and in deference to the need to facilitate the admission of these documents into evidence where continual interaction with similar documenting styles and systems has shown them to be trustworthy. In recognition of this, the Commission accepts the need to continue this exception to the exclusionary rules concerning documentary evidence in order to avoid the difficulties of the practice which formerly required every written document to be authenticated by the individual who prepared it. However such exemptions should not be interpreted so strictly as to deprive the courts of the realities of business and professional practices. Bearing in mind the benefits of the 1879

---

94 He cited in this respect *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 46, discussed above at paragraph 4.98.

95 [1983] ILRM 350.

96 *Gavin v Haughton, Minister for Justice, Equality and Law Reform*, High Court 27 May 2004, Murphy J p 10.

Act, the Commission considers it is important that the proposed statutory framework should retain the essential elements of the 1879 Act, as amended, and that its terms should be extended to include all credit institutions.

4.160 The *Bankers' Books Evidence Act 1879*, as amended, provides that what would otherwise be potentially inadmissible secondary evidence of copies taken from static bankers' records is instead admissible in all legal proceedings as prima facie evidence of the matters referred to in them.[97] As a precursor to this some secondary characteristics of the records must first be established to avoid attracting the rigours of the rule against hearsay. It must be proved that the source document was one of the ordinary business documents of the bank at the time and that the impugned entries were made in the course of these ordinary business transactions rather than in anticipation of litigation and furthermore that the book has been maintained in the possession of the bank.[98] The Commission now turns to summarise its provisional conclusions on this aspect of the law

4.161 The Commission provisionally recommends that the court should retain the discretion to refuse to admit business records.

4.162 The Commission provisionally recommends the retention of the Bankers' Books Evidence Act 1879 (as amended), which should be updated to apply to all credit institutions.

4.163 The formalities of laying a suitable foundation for business and other documents mentioned herein which do not attract the Hearsay Rule are considered in detail in Chapter 5.

4.164 It must be noted that electronic business records prepared specifically for the purposes of litigation ordinarily are not admissible in other jurisdictions such as in the US under the *Business Records Act* or Federal Rules of Evidence, Rule 803(6) because they fail the test of being "created for motives that tend to assure accuracy"[99] but this situation has yet to occur in this jurisdiction.

(5) Concluding Remarks on the Business Records Exemption

4.165 The business record rule was developed at common law, and since then has been replaced or supplemented by statute in most jurisdictions. Generally speaking, if a record is created in the ordinary course of business and is (of a type) relied on in the business, then it is admissible. Some rules require

---

97 Section 3.

98 Section 4.

99 *US v Sanders*, 749 F.2d 195, 198 (5th Cir. 1984).

that it is created contemporaneous to the event recorded, and by a person with a duty to record it. The theory is that these circumstances surrounding the creation of the document lend sufficient gravity to its contents to enable it to be admitted. This is because false or misleading information is unlikely to be recorded on a daily basis where litigation is not foreseen. The mere formalities surrounding the circumstances of the making, retention and the use of the record in the course of business provides a sufficient guarantee of the truth of the document's contents to support admission.

4.166 The business records exemption is presented under a slightly different guise in the US Federal system. This exempts documents from the rigours of the Hearsay Rule which are evidence of regularly conducted activity. This is a wide provision embracing a large spectrum of data compilation instruments and serves to admit them in disregard of the strictures of the Hearsay Rule. This section is vital for the purposes of admitting computer and other electronic or automated evidence whether these present as a

> "memorandum, report, record, or data compilation, in any form, or acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make (that record) all as shown by the testimony of the custodian or other qualified witness".

4.167 An integrity-based safeguard is then inserted operating to legitimate only that evidence where the source or indeed the means or circumstances surrounding the document's preparation lend weight to its credibility. Anything which would seem to "indicate a lack of trustworthiness" loses the shield provided by this section and is excluded.

4.168 A further saving mechanism is included where there has been a deliberate contrivance or oversight which resulted in the exclusion of certain information from the records in accordance with the above provisions and evidence that a matter is not included in the data compilations, is admissible "to prove the nonoccurrence or nonexistence of the matter", which was of a kind which the documentary instrument regularly records. This information is admissible subject to the proviso that it will be excluded where the "sources of information or other circumstances indicate lack of trustworthiness".

4.169 The early manifestation of the business records exceptions to the Hearsay Rule emerged in a business climate when it was still practical and the norm to make manual records in the course of the business enterprise. Today however, with the increasing volume involved this is no longer practically possible. Reliance is now placed on the computer which is capable of indefatigably processing huge volumes of information. Databases and their

master-software have become more complex but also more malleable. Databases are vulnerable to being added to, subtracted from and manipulated. This process may not indeed follow a sinister motive and it may be merely that where databases are replicated and interface between computers is automatic, these computers may not necessarily share the same language and so a degree of translation takes place.

4.170 As a means of saving archiving, man-power and storage costs many organisations keep records in copy form using electronic and digital techniques. Some species of legislation however including tax and company legislation require that original business records be retained and therefore it may be that at the time of litigation the original written document will often be in existence. Where this is so, the common law would require the original be produced. It may, however, be difficult and costly to find it and to get it to court whereas the business could easily and cheaply produce the copy records.

4.171 Business records exemptions were introduced as a shield to guard against the deficiencies of human memory when attempting to recall the classes of records with which they are concerned and in order to allow these documents to be received into evidence. They are in essence self-authenticating with evidential solace drawn from the experienced and repetitive nature of these data collection tools which has conditioned courts to view them as inherently trustworthy. They should be liberally construed to avoid the difficulties of an archaic practice which formerly required every written document to be authenticated by the individual who prepared it. Such exemptions should not be interpreted so strictly as to deprive the courts of the realities of business and professional practices. The formalities of laying a suitable foundation for business and other documents mentioned here which do not attract the hearsay rule are considered in Chapter 5.

CHAPTER 5 AUTHENTICATING DOCUMENTS GENERALLY AND THE LAW OF EVIDENCE

5.01 This Chapter addresses the means by which to authenticate documentary and electronic documentary evidence. In Part A, the Commission discusses the changing landscape of documentary retention practices by looking at the proliferation of digital documentary forms and the emergence of the paperless office.

5.02 Assuming, as the Commission has recommended, that the Best Evidence Rule is to be abolished and the regulation of evidence shifts to a more inclusionary approach, the next step is to establish the authenticity of the documents. In Part B, the Commission examines the cornerstone of authenticity for the purposes of admissibility which is the laying of a suitable foundation upon which to ground evidence. This section questions whether there is a need for the higher standard foundation to be imposed for documentary evidence as is the case in the US as well as other specific evidential requirements for computer-derived evidence. It also discusses the admissibility of business records, digital records (both automated and those generated by human intervention), public documents and on the status of copies as admissible evidence.

5.03 With particular reference to electronic and automated documentary evidence, Part C discusses the different tests which are undertaken in different jurisdictions to ensure the integrity and establish the authenticity of digitally produced information in documentary form and examines whether any of these are appropriate for incorporation into the law of evidence in Ireland.

5.04 Part D addresses the difficulty of categorising electronic and automated documentary evidence which can be real evidence or documentary hearsay depending on the level of manual input and human agency involved. The Commission concludes that where the evidence has been inputted into an electronic database and the device has essentially been used as an electronic filing cabinet the admissibility of the evidence can be determined in accordance with the rules governing hearsay and its exceptions. Difficulties arise where the electronic evidence is automatically generated within the computer matrix of the mechanical device and the knock-on effect this had on the authentication of these documents is analysed.

5.05 Part E examines the means of authenticating public documents where these are intended for use or received from outside the jurisdiction. There is a discussion about the move from legalisation of documents through the use of notarisation and the 1961 *Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents* which replaces domestic legalisation procedures with a streamlined and uniform Apostille document.

A Authenticating Documentary Evidence

5.06 Before it can be admitted in evidence a document, like any other prospective piece of evidence, must satisfy certain minimum standards. These include production, original form, integrity, relevance and compliance with the exclusionary rules. The most prominent of these is to establish the evidence as relevant to the proceedings. The evaluation of the evidence in light of the other factors flows on from this in order to determine the admissibility of the evidence. Where found relevant the discussion then moves towards establishing authentication and apportioning the weight to be attached to the documentary materials. The process of authentication in regard to documentary evidence is a means by which to examine and verify the accuracy and formalities observed in the execution of the document.

5.07 As already discussed in Chapters 3 and 4, certain classes of documents, such as business records or public records, do not need to be authenticated where they are generated or maintained in the course of business or where they bear an official seal or signature.

(1) Production

5.08 For a document's admissibility to be properly addressed it is axiomatic that it must first be produced to the court for assessment. Since the natural state of electronic evidence is a series of bit maps, the law of evidence must make allowance for an output device used as a production tool to ensure the document is available in legible form.

5.09 Issues as to the reliability of the device can be raised as part of the production process while questions which may require oral evidence are more appropriately the preserve of the authentication process.

(2) Original Form

5.10 The Best Evidence Rule, at least in its strict sense, required that unsupported unsworn documentary evidence was not ordinarily admissible to prove the contents of a document unless the original document was itself produced. The difficulties associated with the Best Evidence Rule have been

addressed and resolved in Chapter 2, where the Commission provisionally recommended that it be replaced by a presumptively inclusionary rule.[1]

(3) Integrity

5.11 The integrity of the document ought to be established from the point at which the information was first generated in its final form as a documentary piece of real evidence. In addressing the question of whether the information has been maintained complete and unaltered, the integrity must be sufficiently established.

5.12 This is particularly relevant in determining the origin and author of the document or the participant in a transaction traced through the document and the means of assigning these in a predictable manner which promotes confidence and trust in the documents relied on. In this way authentication can be seen as a process which considers a continuum of risk.

(4) Authentication of Electronic and Automated Documentary Evidence

5.13 The process of authenticating electronic and automated documentary evidence can vary depending on the level of security required and the vulnerability of a given document to spoliation or fraudulent interception and consequent alteration.

5.14 The means of establishing this can be supplemented by a thorough records management system where access to documents is protected and recorded. This can be accomplished through the use of a basic single-factor authentication requirement making use of a simple user name and inputted password issued through secure channels and which is kept confidentially. There is also the option of a two-factor authentication scheme including challenge-response protocols or Public Key Infrastructure (PKI) certificates[2] involving registration or electronic notarisation. There is also the possibility of using a high-factor authentication process utilising secure personal identification techniques and advanced electronic signatures or biometrics.

5.15 The choice of security mechanisms which an individual or undertaking will opt for to safeguard their documentary materials is based on the risks inherent in the particular device and the level of security required.

(5) The Emergence of Electronic Documents

5.16 At its most basic level an electronic document is made up of representative bitmaps which translate illegible data messages into a visible

---

1 See paragraph 2.153 above.

2 See Chapter 7.

and cogitative format. A bitmap is a representation, consisting of rows and columns of dots of an image (this is usually a graphics image) in computer memory. The value of each dot is stored in one or more bits of data. The density of the dots, the resolution, determines how sharply the image is represented. To display a bit-mapped image on a monitor or to print it on a printer, the computer translates the bit map into pixels (for display screens) or ink dots (for printers). Optical scanners and fax machines work by transforming text or pictures on paper into bit maps.

5.17 To ensure the evidential validity and maximise the value of documents which are introduced in evidence, they must first pass over a series of evidential hurdles. One of the most significant of these it that the court must ensure that the evidence meets the test of admissibility. To pass this test it must be relevant and be positively identified as authentic and unaltered.

5.18 The means by which the admissibility of a digital document can be shown is difficult to define and has been described as a moving target.[3] Electronically produced evidence is viewed as suspect owing to the perceived ease with which is can be altered and so precautionary measures must be taken to ensure that electronic and automated documentary evidence has not been tampered with, erased, or added to. These precautions include examining the foundation as well as authentication requirements to establish the integrity or otherwise of the impugned document.

5.19 The Commission provisionally recommends the adoption of an inclusionary approach to the admissibility of both manual and electronic documentary evidence, subject to a number of safeguards and the continuance of the discretion of the court to exclude the evidence.

5.20 Adopting an inclusionary approach to admitting documentary evidence would acknowledge a far more efficient and realistic evidential regime. Safeguards, strictly observed would act as gate keepers to ensure that false and misleading evidence would be excluded.

(6) The Changing Evidential Environment

(a) The Onset of the Paperless Office and the Resulting Proliferation of Computer Records

5.21 The traditional notion of document retention is one of storage of sheets of paper in, for example, filing cabinets. This idea has begun to fade. Space and funds are finite and the physical storage of paper is no longer a cost effective means of warehousing data records. When storage areas are full, a

---

[3] *Computer Crime Investigation and Computer Forensics, Information Systems Security*, Summer 97, Vol 6 Issue 2, p56.

choice must be made either to destroy and lose the data or take older records out and file them away in boxes. Additional space is rented "off site" just to store old records, restricting access to documents and information. This leads to waste and expense desirable in neither the public nor private sectors.

5.22 This has resulted in the gradual onset of the paperless office and flowing from this there has been a proliferation of electronic document generation and storage methods. Documentary imaging services (out sourcing) and turn-key solutions (in sourcing) cheaply convert original "source" paper documents into electronic images where the image is scanned, compressed, indexed and transferred to another medium such as a compact disk, optical disk or hard drive for storage.

5.23 It is estimated that the average employee sends 20 and receives 30 emails daily[4] and that over 80% of all corporate data is created and stored electronically without ever being converted to paper.[5] Another source estimates that 93% of all business documents are created electronically and only 30% are ever printed to paper.[6]

5.24 Electronically generated and stored information is uniquely durable and is not amenable to the shredding process which so easily frustrates the admittance of traditional paper records. In the United States, it has been noted that in the event of the loss of the electronic records, "essential transmittal information relevant to a fuller understanding of the context and import of an electronic communication will simply vanish."[7]

5.25 The retrieval and discovery of a document, however, produces more challenges. Most indexing of digitally stored documents is done through tagging a document, transforming it to an Optical Character Recognition (OCR) format. This translates and customises each character on the document and incorporates it within a master index allowing a search of the documents by any

---

4 Lyman & Varian, *How Much Information?* 2003, http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/ (study of electronic information by faculty and students at the University of California at Berkley School of Information Management and Systems).

5 Jones, *What a Mess! For Corporations, Pileup of Electronic Data Could Be Trouble Waiting to Happen*, NAT'L LJ, Dec 2, 2002, at C6, taken from Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence, Oregon Law Review,* Vol 86, 1201 at 1207.

6 Lange, "*Sarbanes-Oxley Has Major Impact on Electronic Evidence*, "National Law Journal, January 2, 2003, http://www.law.com/jsp/article.jsp?id=1039054510969.

7 *Armstrong v Executive Office of the President*, 810 F Supp (DDC 1993) at 1280.

Boolean search or trawl for a key word, date, account number or other relevant matter. The retrieved document is an exact representation of the original scanned document and is totally unalterable, thereby preserving the integrity of the document. All of these scanned and indexed documents are combined with the company's electronic claim file, payment logs, activity logs, e-mail records and the like leading to an entirely electronic file which can be managed, retrieved, organised and utilised much more efficiently and cost-effectively than its counterpart paper file can be.

B Laying a Suitable Foundation for Authentication- the Cornerstone of Admissibility

(1) Documentary Evidence; Overcoming the Oral Tradition for the purposes of Admissibility and Authenticity

5.26 In its 1980 *Working Paper on the Rule against Hearsay*, the Commission stated that "legal rules must be framed to take account of … technological developments."[8]

5.27 A significant difference between the application of the hearsay rule to oral and written statements is that written and documentary statements must adhere to certain requirements before a document can be admitted in evidence. These requirements mean that the proffering party must prove the contents of the record by producing the original or, in certain circumstances, by adducing a copy or other secondary evidence of the contents. The party must then prove the authenticity of the disputed record. It must also be noted that compliance with these requirements will not relieve the party of the burden of complying with the hearsay rule. [9]

5.28 Tangible evidence has been a key feature of court proceedings for centuries, and represented a means of introducing evidence to the court which was in turn subject to testing by oral cross-examination. The courts consider that the demeanour of the party is of significance in determining the authenticity of the impugned document and whether it was deemed admissible. This was the accepted mode of testing documentary evidence for centuries before the advent of electronic (and especially computer) documentary evidence, which has been a relatively recent phenomenon.

5.29 Traditionally direct oral testimony has made up the cornerstone of testimony in legal proceedings. The necessary corollary to this was a reluctance

---

8 LRC WP No. 9 1980, p 82.

9 See *The People (DPP) v Byrne* [1987] IR 16 where this distinction was initially laid out.

to rely upon information contained in documents prepared by parties other than those directly involved in litigation and which were refused admissibility on the basis of the rule against hearsay. The traditional evidential rule in relation to documents is that a party wishing to rely upon the truth of the contents of the document must call the person who made the document to prove the truth of the facts stated.

5.30 With the proliferation of the paper-less office and the near saturation of electronic means of communication, it is becoming increasingly difficult to operate with records and information that are not stored on computers in some form. In an increasingly technologically-oriented society, computers are used to conduct a wide range of functions across both public and private spheres. As a means to this end, the vast majority of information that was previously calculated and stored on paper now exists exclusively on computers.

5.31 The consequence of such a shift in how information is collated and communicated is that electronic or automated documentary evidence is an increasingly visible element of litigation.[10] Areas as diverse as commercial litigation, criminal fraud prosecutions, and bankruptcy proceedings are examples of the legal fields that frequently involve computer records as evidence. Questions as to the admission or exclusion of computer documents into evidence have gained importance and represent a significant crutch or barrier to the eventual resolution of the case.

5.32 Nicoll is of the opinion that "owing in part to the mystique that still surrounds computer technology even at its lower levels of complexity, computer evidence is powerfully persuasive. Many, including judges and jurors, adopt the attitude that one cannot argue with science. In doing so they suspend their critical faculties and attribute to the computer a status it does not deserve."[11] The reliability and trustworthiness of computer records is thus a key matter to determine.[12]

(2) The Rule Against Hearsay as a Barrier to Admissibility of Documentary Evidence

5.33 The long-standing evidential barrier to admitting evidence in documentary form was affirmed for the purposes of English law in *Myers v*

---

10 Johnson, "*Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability*," 75 Marq L Rev 439, 439 (1992).

11 Nicoll. "*Should Computers be Trusted? Hearsay and Authentication with Special Reference to Electronic Commerce, Journal of Business Law",* 1999.

12 Peritz, R. *Computer Data and Reliability: A Call for Authentication of Business Records under the Federal Rules of Evidence*, 80 NwUL Rev 956, 957 (1986).

DPP.[13] In that case the trial judge permitted the introduction of evidence in the form of documentary records compiled during the assembly of certain cars alleged to have been stolen. The assembly line workers compiled the records by copying the cylinder block number and the engine and chassis numbers onto a card accompanying each vehicle. The information on these cards was then transferred to microfilm and the cards were then destroyed, and the microfilm placed in the manufacturer's records. In an effort to prove that the disputed motor cars being sold were in fact reconstructed stolen vehicles, the prosecution called an employee of the manufacturers to give evidence. The witness produced a micro-film of documents which had been completed by a number of unidentifiable employees of the car manufacturing company which showed that the numbers stamped on the cylinder blocks of the cars which had been sold were the same as the numbers on the cylinder blocks of the stolen cars.

5.34 On appeal following the defendant's conviction, the House of Lords held that the evidence was inadmissible as hearsay given that "[t]he entries on the cards were assertions by the unidentifiable men who made them that they had entered numbers that they had seen on the cars."[14] Thus the only way the evidence could be introduced would have been by producing witnesses whose uncertain recollections would have been of little practical use.

5.35 The House of Lords continued on this path for excluding documentary evidence in the absence of supporting oral testimony in *Gillespie*[15] where Winn LJ stated that:

> "… it is not competent to prove a fact against an accused person by producing a document in which that fact is recorded without calling the maker of the document to say that what he wrote in the document represented a true statement of fact".[16]

5.36 These cases motivated the introduction by the UK Parliament of the *Criminal Evidence Act 1965* which took an inclusionary approach to such evidence. The Commission now turns to examine whether the *Myers* approach should in general continue to apply in Ireland. In this respect, the important distinction must be made between the approach to the admissibility of documentary evidence where adduced as proof of the contents, as in the *Myers* case, and the approach to admissibility in the narrower context of admissibility

---

13 [1965] AC 1001.

14 [1965] AC 1001 at 1002 as per Lord Reid.

15 (1967) 51 Cr App R 172.

16 (1967) 51 Cr App R 172 at 176.

for the purposes of merely proving that the document exists. This duality of the roles for which documentary evidence is offered should, in the Commission's view, be legislatively recognised.

(3) Electronic Evidence in Ireland and the Problem of Hearsay v Real Evidence

5.37 The application of the strict rules of evidence to newer forms of evidence be they electronic or automated and the difficulties arising from these has been recognised to the extent that "(i)n leaving paper, we have also left almost all guarantees of authenticity and reliability..."[17]

5.38 It was pointed out in the Irish context in the 1990s that digital documentation must be addressed from an evidential setting.[18] This followed a series of criminal prosecutions which, apparently, failed because of reliance placed on computer printouts. This led to the enactment of the *Criminal Evidence Act 1992* designed to identify the circumstances where computer printouts would be deemed admissible as evidence in criminal proceedings.

5.39 An opponent of electronic or automated documentary evidence may object to its admission on the grounds that it is hearsay. Electronic documentary evidence is, however, real evidence where it is obtained without the intervention of human agency and created instead by the interaction within a digital matrix. Courts in the United States have taken the view that since this type of evidence is "the by-product of a machine operation which uses for its input 'statements' entered into the machine" and which "was generated solely by the electrical and mechanical operations of the computer and telephone equipment," it constitutes real evidence as opposed to documentary hearsay.[19] An example of this can be seen in the American case *State of Louisiana v Armstead*[20] where the court held that electronically generated telephone trace records do not constitute hearsay as they are generated solely by the electronic operation and mechanical pulses of the computer and telephone equipment rather than computer-stored human inputted statements.[21]

5.40 Information obtained from an electronic device, whether printed and reproduced in permanent legible form or produced before the court

---

17 Schmidt and Zeffertt, "*Evidence*", para 133 from Joubert: "*The Law of South Africa*", Volume 9, First Edition, 1997, Butterworths.

18 Dwyer, P. "*The Admissibility of Computer Derived Evidence"*, (1991) 9 ILT 192.

19 *State of Louisiana v Armstead*, 432 So.2d 837 at 839 (La. 1983).

20 432 So.2d 837 (La. 1983).

21 This was approved in 2000 in *State v Carter,* 762 So.2d 662 (La Ct App 2000).

electronically and read out from a display terminal, can be divided into three categories.

5.41 The first is where the machine is employed as a mere computational device to process information. Here the machine operates with significant human input and the resulting documents are traditionally viewed as documentary hearsay evidence. As is the case with other hearsay statements, admissibility in these cases is subject to the hearsay rule. This means that where the electronic documents are admitted in order to prove the truth of the matters contained therein, the offering party must satisfy the court that the human input and statements identified are: reliable, accurate in the information they display and authentic.

5.42 The second category of documents is comprised of information the computer has been programmed to record automatically without human interference. The resulting information is automated electronic evidence and is seen as real evidence and admissible as such.

5.43 In *R v Coventry Magistrates Court*[22] printouts were made from a web server database which had recorded the click streams and access to websites and which had recorded the name, home address, email address and credit card details of those logging on. These were held to be admissible as real evidence.

5.44 The third type of electronic documentary evidence is a hybrid notion of evidence and raises problems for classification and authentication when it is sought to be admitted. This is information which may have been recorded and processed by the machine but which has been entered by a person and is therefore a cross-breed of a computer processing information which has been inputted by a fallible individual. It is hearsay evidence and must be drawn within one of the exceptions to the hearsay rule as it currently stands.

5.45 In respect of these three categories the rules of admissibility operate so as to admit a computer printout in evidence in the following circumstances -

5.46 Where the printout constitutes real evidence, that is, the documentary statement is produced by an automaton and is completely devoid of all human intervention. Created by the mechanical processes of the machine, it can properly be classed as real evidence and admitted accordingly.

5.47 Where the printout does not constitute real evidence but it is admissible under one of the exceptions to the hearsay rule.

---

22 [2004] EWHC 905.

5.48 And with respect to both (1) and (2) foundation testimony establishes that the computer which produced the record is reliable and which is in turn an opportunity to establish the authenticity of the evidence.

(4) Laying a Suitable Foundation for Electronic Evidence

5.49 Questions arise as to whether a more stringent set of evidential requirements ought to be imposed upon electronic documents relative to their presumed corruptibility. The following examination of the law as it stands outlines the different tests and standards which could be imposed. The conclusion reached by the Commission is that while the suspicion is that electronic documentary evidence may appear more malleable, it is not, in fact, more susceptible to alteration and fraudulent misrepresentation any more than paper-based systems of recording information.

(a) Foundation Testimony in Ireland

5.50 An issue representing a major stumbling block to litigants in the current legal environment is where the dominant form the evidence takes is a document in non-legible form stored in a computer memory and reproduced as an imaged document.

5.51 The process of laying the foundation where evidence from a computer is to be adduced in a trial means that the court must decide upon the form in which it is to be tendered and the authenticity of the printout itself. This remains standard evidential practice given that documents in the main do not speak to their own veracity and are not therefore self authenticating. There must instead be foundation testimony as to how it came into existence because a hard drive, or the programme within it, may be unreliable, either by reason of its make and design or by contrivance where it has been tampered with.

(b) Section 6 of the Criminal Evidence Act 1992- Evidence of Admissibility

5.52 The matter of laying the foundation in Irish law was incorporated into section 6 (1)(d) of the *Criminal Evidence Act 1992* which lays out a legislative framework for the certification of documentary records in criminal proceedings. Section 6 of the 1992 Act hinges on the personal knowledge of the person charged with producing the document. It is this personal knowledge which lends credibility to, and acts as an aid for adjudicating on the authenticity and admissibility of any document sought to be adduced in accordance with section 5 of the 1992 Act.

5.53 Section 6 of the 1992 Act allows for the admission of business records by drawing such documents within the inclusionary exception provided. It therefore overcomes the problem to which the decision in the UK House of Lords in *Myers* gave rise. Further protection is aimed at through the requirement

that a certificate be issued by a party occupying a position in relation to the management of the business in the course of which the information was compiled and which attests to the veracity of the document.

5.54 Section 6 of the 1992 Act goes on to state that the certificate "shall be evidence of any matter stated or specified therein". It essentially vouches for the documentation and identifies it as one of a self-authenticating class of document, in the absence of an objection being raised in accordance with section 7(2) of the 1992 Act. Section 7(2) states that any objections to the admissibility of the proposed evidence will not be entertained unless lodged not later than 7 days before the commencement of the trial. Thus, the onus of producing a piece of evidence will be deemed satisfied by the issuing of a certificate under section 6 following which the burden of proving effectively passes to the opposing party.

5.55 Further evidence of the creation of such an unimpeachable and self-authenticating sub-class of documents is visible in section 6 (2) which allows

> "for the purposes of sub-section 1 it shall be sufficient for a matter to be stated or specified to the best of the knowledge and belief of the persons stating or specifying it."

5.56 This seems to negative any objections to the introduction of any documentary evidence from business records despite issues concerning the authority of the witness to adduce the data from the records of a business.

5.57 Section 6(2) seems to indicate that it is permissible to lodge a certificate which would not require any further verification by the certifier (or person in a suitable position of managerial or other authority from the business whose commercial documents are the subject of challenge). The only opportunity for challenge is under the mechanism provided in section 7 (2) where objections to the admissibility will be entertained to either the whole or any specified part of the information in the certificate. Following such a challenge, the court must require oral evidence to be given of any matter stated or specified in the certificate.

5.58 The provisions in the 1992 Act relating to admitting documentary evidence do, however, contain safeguards. These take the form of a judicial discretion under section 6(3) (a) and (b) by which the court retains a residual discretion to require oral evidence to be given of any matter stated or specified in the certificate. This introduces a system of checks and balances at the behest of the court where the proposed evidence and the manner in which it has been certified is independently assessed.

5.59 The Commission considers that the safeguards in the 1992 Act provide a sufficient level of protection against any likely abuse or fraud concerning the admissibility of such business records. Indeed, the Commission

notes that similar protections gave been put in place in comparable legislative provisions in other jurisdictions.

5.60 In determining the authenticity of a given document it is likely that the court will exercise its discretion and consider the following 6 factors in determining whether the electronic or automated documentary evidence and resulting document is authentic:

- whether the computer was working properly;
- whether the programme in use with regard to the evidence was faulty;
- whether the secondary media (disks, usb keys) upon which the information was stored have been damaged or interfered with in any way;
- whether proper record management procedures were in operation;
- whether error checking mechanisms existed with respect to the original creation of the programme, and;
- whether proper security procedures were in place to prevent the alteration of the information contained in the drive file or secondary storage device prior to the information being reproduced in permanent legible form through a printout.

5.61 The question arises as to whether these criteria should be legislatively imposed or should remain a matter to be considered in an individual case in light of the potentially enormous costs which would have to be invested to determine with any degree of certainty whether the electronic system was operating correctly at a given time.

5.62 The imposition of such a prescriptive provision in an *Evidence Bill* would, it is suggested, be a retrograde step. The Commission do not believe that a more comprehensive prescriptive foundation requirement is necessary to aid in the authentication of computer records as discussed below by the US court in *US v Velo*.

(c) Laying a Foundation in the US

5.63 As with any evidence, the proponent of digital evidence must lay the proper foundation for its admissibility. Courts remain concerned with the reliability of such digital evidence, evidenced by early court decisions in the United States such as *US v Scholle* which established that before a document could be admitted, any process of authentication called "for a more comprehensive foundation"[23] and imposed a greater burden on litigants

[23] 553 F.2d 1109 (8th Cir. 1976) at 1125.

attempting to adduce electronic evidence. Here the US Court of Appeals for the 8th Circuit held that the proponent of electronic evidence must delineate "the original source of the computer program...and the procedures for input control including tests used to assure accuracy and reliability" as part of the foundation to ensure the reliability of the evidence.

5.64 This approach was followed by the Court in *United States & Fidelity Guaranty Co. v Young Life Campaign, Inc*[24] which concluded that the foundation for computer records, while similar to that for other business records, required "special application".

5.65 Over time the strictness of this rule was relaxed and US courts have since rejected the notion that the party seeking to adduce electronic documentary evidence must satisfy a heightened "foundation requirement". In *US v Vela* the US Court of Appeals for the 5th Circuit upheld the trial court's admission of electronic evidence despite the proponent's foundation witness failing to identify the type of computers used to generate the records and who did not verify the computers as being in proper operating condition.[25] The Court explained that "[t]he failure to certify the brand or proper operating condition of the machinery involved does not betray a circumstance of preparation indicating any lack of trustworthiness."[26] The Court proposed that the challenger could argue that the records were unreliable and unbelievable after the records had been admitted, thus attempting an all-embracing inclusiveness in its approach to admitting evidence.

5.66 As courts, became more familiar with digital documents, they withdrew from the requirement of a higher standard with the result that the

---

24 553 F.2d 1109 (8th Cir. 1976) at 1125.

25 *United States v Vela*, 673 F.2d 86, 90 (5th Cir. 1982); see also *United States v Moore*, 923 F.2d910, 914 (1st Cir. 1991) (finding that the head of the bank's customer loan department is a competent foundation witness for computerised consumer loan records compiled by an independent service bureau which is connected to the bank via telephone); *United States v Bonallo*, 858 F.2d1427, 1436 (9th Cir. 1988) (rejecting the argument that computer records are inherently untrustworthy, and, thus, inadmissible, because they can be altered); *People v Lugashi*, 252 Cal Reptr 434, 440-443 (Cal Ct App 1988) (admitting computer records under the business records exception to the hearsay rule does not require testimony from a computer expert as to the computer's technical reliability).

26 *United States v Vela*, 673 F.2d at 90.

courts in the US as demonstrated in *US v Vela* have since held "computer data compilations… should be treated as any other record."[27]

5.67 Although these later decisions indicate some reduction on the foundation requirement, it appears that the "more comprehensive" foundation required by *Scholle* remains a requirement in some courts in the United States.[28] The American Law Reports have summarised a number of ways to establish and meet the requirement of the comprehensive foundation and ensure by testing the reliability of the computer equipment, the manner in which the basic data was initially entered, the measures taken to guarantee the accuracy of the data as entered, the method of storing the data and the precautions taken to prevent its loss, the reliability of the computer programs used to process the data, and the measures taken to verify the accuracy of the programme.[29]

5.68 A 2005 decision of the Bankruptcy Appellate Panel for the 9th Circuit suggests that the burden in the US appears to remain high. In *In re Vee Vinhnee*[30] the court adopted a newer, stricter, standard for the authentication of computer records. The case involved American Express, suing as an unsecured creditor in bankruptcy, seeking to have $41,597.63 owed to it excluded from the bankruptcy proceedings. When the matter came to trial, the debtor did not appear, and the court required American Express to introduce evidence to substantiate the debt. American Express offered to produce a witness who would testify "that he was the custodian of records for the monthly statements, that the entries thereupon were made at or about the time of the transactions, and that the records were kept in the regular course of business, and that the regular practice was to maintain the records."[31]

5.69 Arising from a question of designation of "duplicate copy" on the records, the witness testified that the data was maintained electronically. This led the court to state that such documents required a greater burden to be discharged as:

> "the electronic nature of the records necessitated, in addition to the basic foundation for a business record, an additional authentication

---

27 *United States v Vela*, 673 F.2d 86 at 90 (5th Cir. 1982).

28 553 F.2d 1109 (8th Cir. 1976).

29 7 American Law Reports 4th, 8, 2b.

30 336 BR 437 (9th Cir. 2005).

31 *Ibid*, at 441.

foundation regarding the computer and software utilised in order to assure the continuing accuracy of the records."[32]

5.70 On appeal, the Ninth Circuit panel stated that for evidentiary purposes, "the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."[33]

5.71 The Court cited with apparent approval Prof Edward Imwinkelried's 11 step foundation process for authenticating computer records, namely:

1. The business uses a computer.

2. The computer is reliable.

3. The business has developed a procedure for inserting data into the computer.

4. The procedure has built-in safeguards to ensure accuracy and identify errors.

5. The business keeps the computer in a good state of repair.

6. The witness had the computer readout certain data.

7. The witness used the proper procedures to obtain the readout.

8. The computer was in working order at the time the witness obtained the readout.

9. The witness recognises the exhibit as the readout.

10. The witness explains how he or she recognises the readout.

---

[32] 336 BR 437 (9th Cir. 2005).at 442. As the witness knew little about the company's computer systems, the court allowed American Express the opportunity to make a post-trial submission to establish the foundation for the statements. After American Express filed a supplemental declaration, the court refused to admit the statements because it found the declaration insufficient to establish "that the business conducts its operations in reliance upon the accuracy of the computer in the retention and retrieval of the information in question." Therefore, with no concrete evidence that the debt should be excepted, the court found for the debtor. However, the court accepted that had an adequate evidential foundation been laid, it would have found for American Express.

[33] *Ibid,* at 444.

11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.[34]

5.72 In examining these, the court placed emphasis on the fourth criterion, thus indicating that ensuring the accuracy of the data remained central to the issue and was of critical importance to the reliability of the data. To satisfy this criterion information would have to be furnished to the court regarding details of

> "computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging of changes, backup practices, and audit procedures to assure the continuing integrity of the records." [35]

5.73 In employing this 11 step process, the Court in *In Re Vinhnee* hinted at a stricter standard than had previously been articulated by courts attempting to admit computer data into evidence.[36]

(d) The UK Provisions

5.74 As discussed above, in the US the courts do not require a level of "authentication greater than that regularly practiced by the company in its own business activities …"[37] In England the *Criminal Evidence Act 1965* represented the first generation of legislation to address the need to categorically define a "document" for the purposes of hearsay and documentary evidence. This was later replaced by the *Police and Criminal Evidence Act 1984* (PACE) and by the *Criminal Justice Act 1988*.

5.75 In England section 69 of the *Police and Criminal Evidence Act 1984* provided that where it was sought to adduce electronic documentary evidence this would not pass evidential muster until it was shown to the satisfaction of the court that:

---

34 336 BR 437 (9th Cir. 2005) at 446 quoting Imwinkelried, *Evidentiary Foundations* 5th ed. 2002, § 4.03[2].

35 *Ibid,* at 449.

36 Faced with fulfilling such a proviso, the court viewed American Express's offer as insufficient. The proffered declaration contained "no information regarding American Express' computer policy and system control procedures, including control of access to the pertinent databases, control of access to the pertinent programs, recording and logging of changes to the data, backup practices, and audit procedures utilised to assure the continuing integrity of the records," all of which are "pertinent to the accuracy of the computer in the retention and retrieval of the information at issue."

37 *Cross on Evidence*, 7th Ed, p 635.

"(a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;

(b) That at all material times the computer was operating properly, or if not, that any respect which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents."

5.76 In *R v Governor of Pentonville ex p Osman*[38] computer printouts were adduced and it was argued that these were inadmissible in the absence of proof from the prosecution that the computer had been in proper working order at the relevant time. Lloyd J held however that "where a lengthy computer output contains no internal evidence of malfunction... it may be legitimate to infer that the computer which made the record was functioning correctly."[39]

5.77 *R v Governor of Brixton Prison and Another, ex parte Levin*[40] addressed many questions pertaining to the standards for admissibility in England. The House of Lords noted that section 69 of the *Police and Criminal Evidence Act* imposed requirements on computer-produced evidence that were independent of the status of that evidence as hearsay or not.[41]

5.78 Section 69 of the *Police and Criminal Evidence Act 1984* imposed requirements which had to be satisfied in order for the document to be deemed admissible evidence. In essence, it first had to be established by the propounding party that the computer was being used, and was operating properly. This has been judicially approved as a requirement commensurate with the risk involved and is not a particularly heavy burden to discharge. Thus, in *R v Shephard*[42] it was held that the proper operation of the computer could generally be proved by the evidence of a witness, who was not required to be a computer expert, but who was reasonably familiar with the operation of the computer in question.

5.79 The House of Lords went on to hold in *DPP v McKeown*[43] that:

---

38 [1989] 3 All ER 701.

39 *Ibid*, at 727.

40 [1997] 3 WLR 117.

41 The case concerned extradition proceedings relating to a Russian citizen who had been detained pursuant to an order of the Metropolitan Stipendiary magistrate, with a view to his being extradited to the United States. He faced charges relating to perpetrating fraudulent credit transfers by electronic means.

42 (1991) 93 Cr App Rep 139.

43 [1997] 1 WLR 295.

> "[a]ll that section 69 requires as a condition of the admissibility of a computer-generated statement is positive evidence that the computer has properly processed, stored and reproduced whatever information it received."

5.80 Nonetheless, a document which is inadmissible by virtue of its being hearsay is not rendered admissible merely by the satisfaction of the reliability criteria in s 69 of the 1984 Act.[44]

5.81 A hearsay document which satisfies the section 69 criteria may become admissible under the provisions of sections 23 and 24 of the *Criminal Justice Act 1988*, which allow for the admissibility of certain types of hearsay documents.

5.82 In *R v Harper*[45] the entries relied on were of the third category of evidence identified above, namely the hybrid style of electronic documentary evidence. This evidence is not fully automated and involves the computer as a computational tool to process human inputted information.[46] In this case the documents relied on contained information which had been transferred from manually executed cards to computer memory files. These were offered at trial by an officer of the Inland Revenue who had not been involved in transferring the information in dispute and nor was he a computer technician. On appeal, Steyn J held that the evidence ought not to have been admitted in evidence as section 69 had not been satisfied.

5.83 Steyn J noted the difficulties encountered with evidence of this type and that the law had to evolve to keep abreast of technological innovation. He noted that:

> "the law of evidence must be adapted to the realities of contemporary business practice. Mainframe computers, minicomputers and microcomputers play a pervasive role in our society. Often the only record of a transaction, which nobody can be expected to remember, will be in the memory of a computer. The versatility, power and frequency of use of computer will increase. If computer output cannot relatively readily be used as evidence in criminal cases, much crime (and notably offences involving dishonesty) will in practice be immune from prosecution."

5.84 While he may have been in favour of advancing the law of evidence in its application to technological innovation he was guided by pragmatism and

---

44 [1997] 1 WLR 295, at 302.

45 [1989] 2 All ER 208.

46 See above paragraph at 5.44.

the perceived fallibility of the machine when he noted the prevailing concerns as to reliability. "[Computers] do occasionally malfunction. The phenomenon of a virus attacking computer system is also well established. Realistically, therefore, computers must be regarded as imperfect devices."[47]

5.85 Section 69 of the *Police and Criminal Evidence Act 1984* have since been repealed and replaced by section 60 of the *Youth Justice and Criminal Evidence Act 1999.* The 1999 Act established a degree of functional equivalence as between evidence obtained from an electronic source and its traditionally physically generated documentary counterpart. Section 60 on the removal of the restriction on use of evidence from computer records now states that:

> "Section 69 of the Police and Criminal Evidence Act 1984 (evidence from computer records inadmissible unless conditions relating to proper use and operation of computer shown to be satisfied) shall cease to have effect."

5.86 The same general principles and exceptions now apply to all documents. The 1999 Act provides that a presumption now exists that the electronic device producing the evidential document in legible permanent form was working properly at the material time and is admissible as real evidence. This presumption is subject to rebuttal by the production of evidence to the contrary. Should this occur, the party seeking to produce the electronic or automated document in evidence must satisfy the court that the computer was in fact working properly at the material time.

(5) Reform

5.87 The court in the US case *Vinhnee* adopted the 11 point approach suggested by Prof Imwinkelried. His "prism" effect for laying the foundation in order to admit documents implicitly renewed the need to affirmatively authenticate computer records. Instead emphasis was placed on establishing the reliability, accuracy, and system knowledge of the digital devices in question. While the decision in *Vinhnee* has been identified as an important step in the "evolution of the comfort levels of courts with computer records,"[48] the 11 step foundation process is not, the Commission considers, particularly novel. Instead in essence it forms the crux of traditional authentication inquiries in all areas of evidence.

---

47 [1989] 2 All ER 208 at 210.

48 *Shifting the Burden: The Manual for Complex Litigation* (Fourth Edition, Federal Judicial Centre, 2004, available at www.fjc/public/pdf.nsf).

5.88 The Commission would not encourage the introduction of a similarly strict legislatively imposed foundation for electronic documentary evidence along the lines suggested by Imwinkelried.

5.89 While these 11 steps appear relatively undemanding on the propounding party's electronic system relative to the evidential scale of authentication requirements, it may on the other hand place a considerable onus on the party to prove to the satisfaction of the court, that, for instance the requirement that the computer is reliable. This is a difficult standard to comply with given the flux and spectrum within which consistency can be judged.

5.90 These circumstances are made all the more difficult by Imwinkelried's treatment of the differing vehicles for producing documentary evidence, whether traditional paper-based records or electronically automated or stored images. He attempts to develop a potentially unworkable level of cross-elasticity between the two modes of documentary retention, especially in his second step which requires that the computer be reliable. Establishing this would mean lifting non-transferable concepts between the two mediums. It would involve the transfer of concepts and traits such as durability, reliability and stability traditionally associated with physical paper-based records and applying them to electronically-generated or computer stored images.

5.91 An illustration of the need to take a guarded approach to electronics (which confirms the view of computers and networks as inherently unreliable) can be illustrated by the injection of capital into the US securities market during the period 2000–2004. During this period over $40 billion was spent on information security products and services in an attempt to secure computers and networks from infiltration. It has been suggested that, despite such expenditure to secure computer systems, between 5 to 20% of computers in use may be subject to interference by third parties without the knowledge of their legitimate owners and users.[49]

5.92 The Commission does not, therefore, recommend the introduction of a system of regulating the advent of electronic evidence by testing the integrity of the computer system along the lines of Imwinkelried's 11 step process as this would impose too onerous a burden on litigants.

5.93 The burden of specifying criteria for satisfaction prior to evidence being admitted would, in the Commission's view, prove too onerous. Such prescriptive legislation would make it difficult to specify the nature of the authentication technology in such a way that it would not be overtaken by continuous technological advances. Legislative proposals of this sort could also

---

[49] Kuper, "*The State of Security*," IEEE Security and Privacy, volume 3, no 5, pp 51-53, Sept/Oct, 2005.

mean that certain electronic documents which are otherwise admissible would be excluded on the grounds that they were not obtained or produced by an approved technology despite there being no other reason to doubt their reliability.

5.94 Instead, the Commission considers that a less prescriptive approach would provide a suitable level as to admissibility. Indeed, the approach taken by the Northern Ireland Court of Appeal in *Public Prosecution Service v McGowan*[50] appears to involve the correct balance in this respect. The Court suggested that in matters relating to documentary evidence produced mechanically that the rebuttable presumption would be that the device is "operating properly and in working order in the absence of evidence to the contrary. The presumption of the correct operation of equipment and proper setting is a common law presumption.... In the modern world the presumption of equipment being properly constructed and operating correctly must be strong."

C Tests to be Proposed- Testing the Integrity and Reliability of the Electronic System

5.95 The principle on which the Best Evidence Rule is founded is to ensure the reliability and integrity of the record to be produced in evidence. It is easier to identify that an original paper record has been altered than to determine any alteration by the comparison of electronic documents which may have several versions logged. As a follow on from the original mechanism generating the electronic record, there may or may not be any original paper version of the electronic document in existence. Therefore, the means by which to test the integrity of an electronic record has to proceed in another way. Should the focus be on the integrity of the record-keeping system as the vital element in sharp-focusing the integrity of the record? Examination of the data matrix would include investigating all primary drafts of the document as well as the final product created, maintained, displayed, reproduced or printed out by a computer system.

5.96 In Canada, it was suggested in 1994 that, far from seeking a singular "original", the court should instead move towards identifying a "system" and shift "from a dependence upon proof of the integrity of the original business document to a dependence on proof of the integrity of the record-keeping

50 [2008] NICA 13.

system" with the direct consequence that "the Best Evidence Rule loses most or all of its application in this field..."[51]

5.97 This approach has been taken in Articles 2837 to 2839 of the Quebec Civil Code,[52] and in the *New Brunswick Evidence Act on Electronically Stored Documents 1996.*[53] Both these provisions require that the integrity of the records be demonstrated as a condition precedent to admission. This is satisfied by provisions which seek to establish evidence as to the reliability of the computer system that produced the records, although the New Brunswick statute does not say so expressly.

5.98 The New Brunswick statute also requires that the paper originals of imaged documents must have been destroyed in order that the images be admissible. This highlights a statutorily ingrained preference for paper over electronic records so that, where a paper original exists, an electronic derivative will not be acceptable in evidence. This shows a resistance to modern communication techniques, which must be acknowledged as the norm in contemporary commercial communications. It can be argued that the mere fact that imaging has or had a paper original is irrelevant. If the aim is to be that all electronic records are judged by the same standards, the Commission considers that legislation should be neutral with no preference betrayed as to whether original paper records should be retained, provided that destruction

---

51 Chasse, K. "*Computer-Produced Records in Court Proceedings*" [1994] at para 46, Proceedings of the Uniform Law Conference of Canada available at www.ulcc.ca/en/poam2/.

52 Article 2838 presumes the reliability of the record where it is proved that the data entry is carried out systematically, without gaps and is protected against alterations. Such presumption is also made in favour of third parties who seek to admit the record if it is proved that the data entry were part of a business enterprise. Therefore, in some cases, the Quebec Civil Code provisions require the production of evidence relating to the reliability of the system which created the records.

53 *New Brunswick Evidence Act on Electronically Stored Documents 1996*, SNB 1996 c. 52 The New Brunswick statute provides that a print-out of a document is admissible for all purposes, as is the original document, if it is proved that the original document is copied by a process of electronic imaging or similar process and is electronically stored in the course of an established practice to keep a permanent record of the document. Additionally, it must be proven that the original document no longer exists and that the print-out is a true copy of the original document.

was part of the normal course of business and not in contemplation of litigation.[54]

5.99 The Commission now turns to consider what form this "reliability of the system" test should take. Should the reliability of the system fall to be demonstrated when the evidence is to be admitted or after admission and when its weight is to be determined? The integrity of the record to be admitted is relevant on admission and in determining its weight. At which stage should the issue of integrity be primarily determined - admissibility or weight?

5.100 The Commission is of the opinion that in deciding on admissibility relating to documentary evidence the focus should be shifted from rigidly seeking an original to accepting secondary evidence where shown to have sufficient integrity.

(1) Advantages In Favour of an Integrity Test for Admissibility

5.101 Information as to the integrity of the documents is primarily known to the proponent of the evidence and so it would not be an unduly difficult burden on them to have to supply information confirming this when seeking to offer the documents in evidence. However, it could also be seen as unfair to admit where the opponent has no information that would permit a successful challenge where for example he is unacquainted with the proponent's record management system.

5.102 Requiring the proponent to demonstrate integrity at the admission stage would require a basic level of foundation evidence to be put down and which would then be subject to cross-examination. Were the adducing party not required to provide foundation evidence to support the admission of the electronic or automated document, the opposing party would have to call its own witnesses to challenge the integrity of the record. If this were the case,

---

[54] Contrast this with The *United Nations Model Law on Electronic Commerce* which provides (in Article 9(1)):

> (a) in any legal proceeding, nothing in the application of the rules of evidence shall apply so as to deny admissibility of a data message [ie an electronic record] in evidence:
>
> (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

If the Model Law's Article 9(1)(b) may require that any person who wishes to use an electronic image will have to destroy the original and may have to demonstrate that this destruction was reasonable. This would seem unnecessarily restrictive and needlessly destructive of a possibly valid source of evidence for the sake of uniformity.

what type of witness would be available to the opponent? The best available witness with sufficient knowledge who could testify to the integrity of the proponent's system would be an employee of the proponent. This would frustrate proceedings although the need to call foundation evidence is likely to encourage responsible record-keeping since anyone wishing to introduce electronic records would have to be able to withstand cross-examination.

(2) Arguments Against an Integrity Test for Admissibility

5.103 Requiring that the machine which produces the disputed evidence be proven to have been working correctly prior to the admission of evidence was discussed in the English case *Branagan v Director of Public Prosecutions*.[55] Here the defendant appealed a drink-driving conviction which had been based on a blood sample. The challenge was on the basis that it was a requirement that the intoximeter should be shown to be working properly before the evidence of the blood sample was admissible. Simon Brown LJ held that there is "no possible reason why the prosecution should have to prove one way or the other whether the machine was actually working properly. The defendant is, if anything, better off if it is assumed to be working: the option then becomes his as to whether to offer a breath or blood sample and he can elect which to provide."

5.104 Any proposed integrity test for admissibility will create a hurdle and unnecessary expense for litigants given that in most cases the integrity of the records will not be challenged. This could lead to a procedural abuse of otherwise legitimate uses of electronic evidence in litigation, even if there is no serious dispute about the integrity of the records. Tactical considerations will likely lead the proponent to call evidence to support the weight of a record, particularly if the record is challenged by the other party.

5.105 The Commission therefore proposes that the requirements of the Best Evidence Rule be removed entirely from the regulation of electronically generated documentary evidence, and that the law be clarified to ensure that a proponent of an electronic document not be required to demonstrate that the record is an "original". This proposal would be without prejudice to other specific statutory provisions which may expressly or by implication require the production of an original record. The Commission considers that the text of Article 8 of the *United Nations Model Law on Electronic Commerce* may be helpful in this respect. Article 8 states:

> 1. Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

---

[55] [2000] RTR 235.

(a) There exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) Where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

2. Paragraph 1 applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

3. For the purposes of subparagraph (a) of paragraph 1:

(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(3) What Options are Available to Test the Integrity of Electronic and Automated Documents?

5.106 If the current requirements of the Best Evidence Rule were removed, a number of options for a replacement integrity test at the admission stage could be considered. The Commission turns now to discuss these.

(a) Modification of the Secondary Evidence Rule

5.107 In the event that a distinction is maintained as between electronic and traditional documentary evidence on the basis that the Best Evidence Rule still attaches to electronic evidence, the Commission suggests an alternative to modify the operation of the rule. In particular, it may be desirable to clarify what is regarded as an "original" and a "copy" in relation to particular types of electronic records.

5.108 For electronic evidence to be suitably tested and have conclusions drawn on its admissibility, a court might require a full investigation of the electronic system which produced the electronic evidence as well as questioning the method in which this electronic evidence was produced and decide on whether this met any domestic or international standards (comparison with the *UN Model Law on Electronic Commerce* may be of benefit here).

5.109 This approach might, however, prove too onerous a duty to fulfill from a practical perspective as it would potentially mean increasing the burden on record keeping practices at a pre-litigation stage especially where the integrity of the records would not be seriously challenged.

5.110 A second approach would be to require the proponent to notify the opposing party of the intention to produce the evidence in electronic form and to give evidence of the general reliability of the computer system that produced it if the opponent objects to its admission prior to adjudication on admissibility.[56]

5.111 As with the first approach, however, a demand to notify the other party of the intention to produce electronic documents in evidence provides a technical barrier that would be subject to abuse or overly narrow interpretation. It could add unnecessary expense to litigation.

5.112 A third approach would be to require either oral or affidavit evidence of the integrity of the system. This would be supported by a presumption that the computer- generated document is reliable, subject to rebuttal by the party opposing admission challenging the system/resulting document as undependable.

5.113 This requirement of an accompanying affidavit or oral evidence that the electronic system which had responsibility for generating the electronic evidence is reliable has, in the Commission's view, more to commend itself. For example, the proposed legislative framework could provide that it would be satisfactory for an adducing party to make a declaration as to the service history of the mechanisms in question to the effect that the system was working correctly at the relevant time. This could then be accompanied by supplemental evidence which the producing party would furnish to satisfy the court as to the veracity of his assertions. The presentation of such affidavit or oral evidence would raise a rebuttable presumption regarding the integrity of the electronic record. In-depth and technically extensive proof of the system would only become necessary if the court expressed concern for the integrity of the evidence.

5.114 This option would also provide the opponent with the necessary opportunity to cross-examine the proponent or any expert. The Commission considers that the threat of such a cross-examination would motivate a

---

[56] Such a path was suggested by Ed Tollefson in his 1995 article "*Computer-Produced Evidence in Proceedings within Federal Jurisdiction*", [1995] prepared for the Uniform Law Conference of Canada at paragraph 139. But this was rejected as a possibility by the Conference's "Uniform Electronic Evidence Act Consultation Paper", March 1997, at para 40.

systematic and rigorous system of in-house record management by making the proponent legally accountable for the reliability of the system.

5.115 Questions remain concerning this option in particular as to how a party opposing the evidence could rebut a statutory presumption if this was created as to the integrity of the electronic record?

5.116 A fourth option would be to require nothing more than the usual oral evidence to satisfy the requirement of authentication in order to identify the record.

5.117 The Commission has provisionally concluded that either the third or fourth option should be implemented, that is, either a preliminary quality assurance test backed by a presumption or no test at all beyond having a witness identify the record. Either approach would limit much of the potential procedural abuses that might otherwise develop and relieve the proponent of the onus of maintaining documents in a manner which could be interpreted as being in anticipation of litigation.

5.118 While a regulatory framework requiring an accompanying affidavit or oral testimony prior to the production of electronic documentation is not so onerous as to introduce an insurmountable burden on the adducing party the Commission is of the opinion that no unnecessary burdens should be placed on those undertaking records management systems in the ordinary course of their enterprise. This is aimed primarily at ensuring the integrity of the electronic system in use.

5.119 The functional equivalence between electronic and automated evidence and, traditional tactile documentary evidence is also consistent with the Commission's overall approach that there should be a single technology neutral definition of a "document". This is preferable to the possibility of imposing an artificial distinction for deciding between the authentication processes of the two. For this reason the Commission recommends that electronic and automated documentary evidence be admissible by means of secondary evidence where this is shown to have sufficient integrity, including by reference to the electronic record system used.

5.120 The Commission provisionally recommends that electronic and automated documentary evidence be admissible by means of secondary evidence where this is shown to have sufficient integrity, including by reference to the electronic record system used.

5.121 The Commission emphasises that this proposed reform of the law towards an inclusionary approach leaves the courts to determine the very important matter as to whether the evidence is reliable and to then apportion weight to the evidence.

D When is Electronically Derived Evidence Admissible as Real Evidence?

5.122 Once the court is satisfied as to the authenticity of the printout with which it is concerned, it must then consider the question of its admissibility. Case law in the United Kingdom has drawn a distinction between computer derived evidence which is, on the one hand, admissible because it is real evidence and which, on the other hand, is inadmissible because it is hearsay.

5.123 Computer printouts may be admissible if they constitute real evidence. Evidence is real evidence if it is tendered to show the existence of itself as a documentary object. All exhibits produced for inspection or examination by a court are covered by the term real evidence, whether a weapon, a person's physical appearance, or an automatic recording. In the context of electronic or technologically derived evidence the documents in question can be said to be real evidence or direct evidence where they are used circumstantially rather than testimonially so that the form that the evidence takes is relevant and it is introduced as evidence as proof of itself and the fact that it exists rather than as proof of the facts asserted in it which would render it documentary hearsay.

(1) Real Evidence in Ireland; The Hearsay Question

5.124 The *Criminal Evidence Act 1992* involved a fundamental reversal of the rule against hearsay by providing for the admissibility of business records in criminal proceedings, subject to certain conditions. They can be introduced by means of a certificate of assurance as documentary evidence or by means of oral evidence where that information is tendered by a person who occupies a position in relation to the management of the business or is otherwise in a position to give that evidence.

(a) Specifications as to Computer Based Evidence

5.125 With the emergence of paperless offices, increased computerised communication and issues as to storage and warehousing, many commercial entities now seek to retain data in digital documentary form. These may form a species of either documents retained in a digital form which are inputted and interfaced with a machine or automated documentation which has been generated electronically without human intervention.

5.126 The focus of the 1992 Act is primarily towards documentary evidence of the second category, that is, data involving the interaction of computer systems with human assistance. Nonetheless, automated and computer-generated evidence also falls within the ambit of the 1992 Act and it allows both automatic and manually inputted documentary material to be admitted in evidence.

5.127 The Commission is of the opinion that there is no need for a legislatively imposed parallel process by which to determine the admissibility of electronic and technologically derived documentary evidence in proceedings. There is no empirical evidence to suggest that electronic evidence is likely to be less accurate than paper based documentation, which are as amenable to spoliation and degradation with the passage of time or an extending chain of custody. Where it is alleged that the document has been altered, the document remains admissible as evidence and the alleged discrepancy or fraudulent interception goes to the weight of the evidence rather than admissibility. This is to be resolved by shifting the focus to the authentication of the document.

5.128 In estimating the evidential weight to be given to documentary evidence, a single set of provisions could be more readily employed to legislate for both traditional and electronic and automated documentary materials adduced in evidence rather than attempting two separate evidential regimes. The process of apportioning this weight would mean examining the circumstances surrounding the generation of the document. This would include whether the document was generated contemporaneously with the event or information which it records in the statement, whether the person supplying the information was the creator of the data or merely the conduit for it and whether that person was likely to have been creditable.

5.129 Section 8 of the *Criminal Evidence Act 1992* incorporates a judicial discretion to exclude evidence which would otherwise be admissible under section 5 where the court is of the opinion that it ought to be excluded in the interests of justice.[57] The factors to be taken into consideration when determining the admissibility and weight of the document include having regard to the overall status of the document from which inferences could be drawn as to the accuracy and viability of the document.[58] Other facets to be weighed include:

> "(a) whether or not, having regard to the contents and source of the information and the circumstances in which it was compiled, it is a reasonable inference that the information is reliable,
>
> (b) whether or not, having regard to the nature and source of the document containing the information and to any other circumstances that appear to the court to be relevant, it is a reasonable inference that the document is authentic, and
>
> (c) any risk, having regard in particular to whether it is likely to be possible to controvert the information where the person who supplied

---

57 *Criminal Evidence Act 1992* section 8(1).

58 *Ibid,* section 8(3).

it does not attend to give oral evidence in the proceedings, that its admission or exclusion will result in unfairness to the accused or, if there is more than one, to any of them."

5.130 The Commission considers that these considerations are sufficiently thorough to be incorporated into the proposed statutory framework which would, of course, extend this approach to both civil and criminal proceedings.

5.131 Questions as to the accuracy of documentary evidence are equally applicable to both paper-based and electronic documentary evidence as with questions which arise from authentication. They apply to the document where it is presented as proof of itself where offered as real evidence rather than where it is adduced as proof of the evidence of its contents (documentary hearsay).

5.132 This is also the case with regard to authenticating documents where the same standards can be applied to both halves of the documentary evidence whole. Authenticity can be proven through oral or circumstantial evidence and equally through exploration of the technical features of the electronic device in question. Paper-based documents are amenable to authentication by the author by attaching a signature or seal. Electronic evidence is also capable of authentication in this way and the chain of custody can also be documented by the use of numerous technological innovations including electronically notarised and certified electronic signatures and passwords or biometric readings.[59]

5.133 In recognition of these similarities, the Commission considers that there can be no basis for artificially dividing the regulation of documentary evidence along the lines of electronic and paper lines, given that where a document is adduced as either real evidence or documentary evidence, the tangible reproduction of the image the physical document - is indistinguishable from the paper document generated on a typewriter.

5.134 The law of evidence as it applies to documentary evidence should adopt a technology-neutral approach, in which the essential rules of admissibility should apply equally to traditional forms of manually created documents and to electronic and automated documents and records.

(2) Digitally-Born Records

5.135 The question as to the status of computer-derived and wholly automated documentary evidence has come increasingly to the fore with the proliferation of e-communication techniques and businesses operating on the premise of speed and documentary dexterity. What then is the status of this information with regard to admissibility and authentication prior to having it introduced as evidence in litigation?

---

[59] See Chapter 7.

(a) The Reliability of the Computer Process

(i) Automated Witnesses

5.136 There can be no doubt that there is now no discernable difficulty with admitting banking records as admissible documentary evidence in the form of a financial institution's computer records. In Ireland these are admissible in evidence following the amendments to the *Bankers' Books Evidence Acts* by section 131 of the *Central Bank Act 1989*, which extended the meaning of "bankers' books" to include computer records within the category covered by the Act and accompanied by oral testimony as to the overall working conditions and reliability of the system. What of situations where there is no testimony available and where the witness is a machine? This may occur in electronic fund transfers through, for example, an Automated Teller Machine (ATM). It is possible in these transactions that computer error may cause a withdrawal to be recorded in circumstances where none occurred. This is termed a "phantom withdrawal."[60] Here, the bank's "witness" is a machine although this may also be accompanied by evidence as to the correct operation of the device at the material time of the transaction.

5.137 How is the unexplained transaction to be explained by the unsubstantiated word of a machine without falling foul of a renewed argument based on the approach taken by the UK House of Lords in *Myers v DPP*? In the US case *Judd v Citibank*[61] the card holder discovered her account to have been debited $800, a transaction she denied having made. The New York Court of Appeals placed the veracity of her testimony above the evidence of the computer printout adduced, owing to the presumed fallibility of the electronic device which it said was wont to break down.

5.138 In the later case *Porter v Citibank*[62] the Court favoured the argument of the oral testimony over the computer printout although here the appellant's position was buoyed by testimony from a bank employee who stated there had been a defect in the computer which recorded withdrawals. Although the quality of the defect related to a different matter and concerned money being dispensed to the next customer this did not prejudice the testimony offered.

5.139 Where the documentary business records in question have come into being through purely mechanical processes and have been generated without direct human facilitation, it can be argued that these form a genus of material

---

60 Banking Services: Law and Practice Report by the Review Committee 1989 (the Jack Report) 7 Cmd 622 (HMSO: London, 1989), pp 83 and 84.

61 435 NYS 2d 210 (1980).

62 472 NYS 2d 582 (1984).

which can be correctly classed as real evidence and which is not then excluded as being contrary to the rule against hearsay.[63] In essence it is not an instrument which has merely recorded a statement. Instead it has gone further and actually created the statement independently of its programmer. When seeking to have this style of documentary evidence admitted, questions arise as to whether this is inadmissible as hearsay evidence. In fact, because the documentary statements originate not in the mind of an individual but in the matrix of an electronic device, the statement may be admissible to prove that which it asserts.

5.140 This approach is supported by the English case *The Statue of Liberty*.[64] Here the English High Court recognised documents as admissible evidence which had been developed in isolation from human input. This involved data from a radar station which had recorded echoes from two ships which had collided at sea. The Court rejected the contention that the data film was hearsay. It was held to have been automated but real evidence and was deemed acceptable on a par with direct oral testimony. Though dating from 1965 the case has continuing relevance for the introduction of other digitally derived evidence such as automatic bank transfers, the logs from telephone and mobile telephone calls as well as automated computerised transactions with the court holding that the same principle would apply to all other types of recordings.

5.141 The decision is authority for the proposition that where information is recorded by mechanical means without the intervention of a human mind the record made by the machine is admissible in evidence, provided of course, it is accepted that the machine is reliable.[65]

5.142 The *Statute of Liberty* decision followed the approach of the English Court of Appeal in *R v Maqsud Ali*[66] which had dealt with the admissibility of audiotapes. The Court noted that:

> "For many years now photographs have been admissible in evidence on proof that they are relevant to the issues involved in the case and that the prints are taken from negatives that are untouched.

---

63 "Real evidence is evidence afforded by the production of physical objects for inspection or other examination by the court". Cockle's Cases and Statutes on Evidence, 10th ed, 1963 p 348.

64 [1968] 2 All ER 195.

65 Smith. *"The Admissibility of Statements by Computer"* (1981) Crim Law Rev 387, at 388.

66 [1965] 2 All ER 464.

> The prints as seen represent situations that have been reproduced by means of mechanical and chemical devices...We can see no difference in principle between a tape recording and a photograph. In saying this we must not be taken as saying that such recordings are admissible whatever the circumstances, but it does appear to this court wrong to deny to the law of evidence advantages to be gained by new techniques and new devices, provided the accuracy of the recording can be proved and the voices recorded properly identified; provided also that the evidence is relevant and otherwise admissible, we are satisfied that a tape recording is admissible in evidence. Such evidence should always be regarded with some caution and assessed in light of all the circumstances of each case."

5.143 The English High Court in *Statute of Liberty* was of the opinion that the contents of a tape recording were similar in principle, as regarded questions of admissibility, to a photograph if properly proven in evidence. Sir Jocelyn Simon P stated that:

> "If tape recordings are admissible, it seems equally a photograph of radar reception is admissible as, indeed, any other type of photograph. It would be an absurd distinction that a photograph should be admissible if the camera were operated manually by a photographer, but not if it were operated by trip or clock mechanism. Similarly, if evidence of weather conditions were relevant the law would affront common sense if it were to say that those could be proved by a person who looked at a barometer from time to time but not by producing a barograph record. So too with other types of dial recordings. Again, cards from clocking-in and out machines are frequently admitted in accident cases. The law is bound these days to take cognisance of the fact that mechanical means replace human effort".[67]

5.144 Similarly, in *R v Governor of Brixton Prison and Another, ex parte Levin*[68] the UK House of Lords noted that it was a "rather spurious notion that a computer-produced document merely appears to assert its contents". The way to adjudicate on that was to determine whether the statement in question was generated through, or in the absence of, human agency. Where documents represent the end-product of a process which did not require the active intervention of a human mind they constitute real evidence. The House of Lords held that where a bank's computer automatically transfers funds from one

---

67 [1968] 2 All ER 195, at 196.

68 [1997] 3 WLR 117.

account to another a printout of the record is not hearsay as to whether a transaction occurred. Instead, crucially, it is a record of the transfer itself.

5.145 Where tape recordings or examples of documentary recording are recorded through the use of computerised compilation billing it is practical to consider that such a document maintained and compiled by a mobile telephone company constitutes "real evidence". There may be certain aspects of the information stored by the company which require human input, but once the process itself has been commenced each automatic transaction which takes place without the need for human involvement, constitutes "real evidence" and its admissibility is not governed by the rule against hearsay.

(ii) Automated Telephone Records

5.146 The position of electronic evidence as real evidence was cemented in *R v Spiby*[69] where the English Court of Appeal held that the trial judge had properly admitted evidence of computer printouts of a machine which had monitored hotel guests' phone calls. Taylor LJ referred to the earlier case of *Minors and Harper*[70] and confirmed that this "was not a printout which depended in its content for anything that had passed through the human mind"[71] and so was admissible as real or direct evidence. The court also noted here that unless there was evidence to the contrary the court would assume that the electronic device generating the evidence was in working order at the material time.

5.147 Taylor LJ remarked though that had the numbers been manually entered into a computer then these would not have attracted the tag of "real evidence". In such a case sections 68 and 69 of the *Police and Criminal Evidence Act 1984* would have applied insofar as they create an exception to the rule against hearsay.

5.148 The limits of the reasoning in the *Statue of Liberty* were exposed in *R v Pettigrew*[72] where the English Court of Appeal refused to apply the earlier decision. Here the prosecution sought to tender in evidence a printout from a machine which was used to record the numbers on bank notes which it had counted in an effort to establish that a quantity of bank notes found in the possession of the accused came from a batch which had been stolen from the Bank of England.

---

69 (1990) 91 Cr App R 186.

70 (1989) Cr App R 102 where Steyn LJ referenced an article by Smith, "*The Admissibility of Statements by Computer*" (1981) Crim Law Rev 387, at 388.

71 Taylor LJ (1990) 91 Cr App R 186 at 191.

72 [1980] Crim Law Rep 239, (1980) 71 Cr App Rep 39.

5.149 A manually inserted code input from a human operator provided the number of the first note. The machine then automatically recorded the rest. The prosecution argued that the printout was admissible under the *Criminal Evidence Act 1965* as being a business record. Section 1 (1) of the 1965 Act required that in order for such a record to be admissible the supplier of the information must have or be reasonably supposed to have had personal knowledge of the information supplied. Because the operator in this case did not have the requisite knowledge of the individual notes given the volume in question the court rejected the evidence as being hearsay.

5.150 This led to some uneven results. For instance in *R v Wiles*[73] which concerned an automatic record made by a meter in an automatic petrol vending system though no computer was involved. Judge Allen held here that the document produced by Wiles at the beginning and end of his shift recording the amount of petrol sold was not a record generated with information supplied by that party. Instead it was supplied entirely by the electronic pump system and did not satisfy section 1 (1) of the *Criminal Evidence Act 1965*.

5.151 It can be argued that the decision highlighted a marked reluctance on the part of the judiciary to extend the principles applicable to automatic recordings to computers, though this has now been overtaken.[74] *R v Wood* involved an appeal from a conviction for handling stolen metals. The identification of the metals was done through cross-checking the chemical composition of the materials on a computer with the aid of human input. At the trial the evidence was not treated as hearsay. Rather it was accepted as real documentary evidence whose relevance and veracity depended upon the expert evidence of chemists to place it in context, and computer programmers to testify as to the operational capacity of the machine. However the documents were held inadmissible as business records as having been generated in anticipation of litigation.

5.152 In England it is now well established that computer printouts are admissible if the computer has compiled the information without the intervention of the human mind provided that the court accepts the computer was properly operating at the time it recorded the information and at the time it produced the printout.

5.153 The dividing line between a document which is inadmissibility as hearsay and a piece of evidence which is inadmissible although it is real evidence may, however, be difficult to draw. The extent to which a computer

---

73 *R v Wiles* [1982] 76 Crim LR 669.

74 In *R v Wood* (1983) 76 Cr App Rep 110; *Pettigrew* was distinguished on the basis that it was a decision confined to the application of the 1965 Act.

uses its memory, or processes information which it has automatically recorded, or depends upon a specific programme to perform a calculation are all relevant considerations which a court must take into account in making its decision as to where to draw the line.

(3) Authenticating Electronic and Automated Documents as Admissible Evidence in Ireland

(a) The Criminal Evidence Act 1992

5.154 Section 6 of the *Criminal Evidence Act of 1992* allows data recorded in documents to be introduced into evidence in the context of criminal proceedings where this information had been compiled in the ordinary course of business subject to the strict criteria of the statute.[75] Section 4 of the 1992 Act sketches a wide definition of a "business" as "including any trade, profession or other occupation carried on for reward or otherwise either within or without the state and includes also the performance of functions by or on behalf of:

> (a) Any person or body remunerated or financed wholly or partly out of monies provided by the Oireachtas;
>
> (b) Any institution of the European Communities;
>
> (c) Any national or local authority in a jurisdiction outside the State; or
>
> (d) Any international organisation."

5.155 This expansive definition includes not merely commercial businesses but also covers the activities of those persons and bodies financed by public monies as well as those funded by international or European Community institutions.

5.156 As to records held outside the State section 5(3) of the 1992 Act states that the provisions of section 5(1) do not apply to information from a party who would not otherwise be compellable at the behest of the party wishing to gain access to data under the Act. The Commission calls for submissions as to whether the proposed rule concerning the admissibility of documentary evidence should apply to information supplied by a person who would not be compellable to give evidence at the instance of the party wishing to give the information in evidence.

5.157 The Commission invites submissions as to whether the proposed rule concerning the admissibility of documentary evidence should apply to information supplied by a person who would not be compellable to give evidence at the instance of the party wishing to give the information in evidence.

---

75 *Criminal Evidence Act 1992*, sections 5 and 6.

5.158 Section 5 of the 1992 Act is the means by which to ensure the admission of documentary evidence in criminal cases and authorises documentary evidence to be adduced where the data it contains is evidence of any fact therein, of which direct oral evidence would be admissible. Admissibility is subject to requirements that the documentary data be shown to have been (a) compiled in the ordinary course of business, (b) supplied by a person (whether or not he so compiled it and is identifiable) who had or may reasonably be supposed to have had personal knowledge of the matters dealt with and (c) in the case of information in non-legible form that has been reproduced in permanent legible form, that it was reproduced in the course of the normal operation of the reproduction system concerned.

5.159 Section 5(1) is applicable whether the information was supplied directly or indirectly with the proviso that if supplied indirectly it will only be deemed admissible where the party, identifiable or not, through whom it was supplied had received it in the ordinary course of business transactions.

5.160 Section 5(4)(b) of the 1992 Act permits the introduction as admissible evidence of a wide variety of documents including data in the form of maps, plans, drawings photographs, or directions given by a member of An Garda Síochána or a record of the receipt, handing, transmission, examination or analysis of anything by any person acting on behalf of any party to the proceedings or a record by a registered medical practitioner of an examination of a living or dead person and permits the admittance of documents as evidence which purport to record evidence of documents in transit.[76]

5.161 Section 5 also permits the presentation of explanatory information which would otherwise be unintelligible. This involves data introduced to account for and place in context data contained in documentary form which would be admissible within the confines of section 5 but which is in form or in terms which are not readily accessible or intelligible to the average person without an adequate explanation. To be admitted pursuant to this provision the person who may be called to give that explanation must be "competent to do so" or, where contained in a document his competence will be deemed established where the document purports to be signed by such a competent person.[77]

5.162 It has been suggested that these provisions are reliant for their admissibility upon the certificate provisions of section 6 of the 1992 Act itself.[78]

---

76 Section 5 (4)(b)(iv).

77 Section 5 (6).

78 Murphy, S, "The Use of Business Records in Prosecutions", (2004) 14(1) ICLJ 19.

5.163 Section 5 can be described as prescriptive in its applicability. While it embraces broad definitions of "document" and "business", it also contains some limiting exceptions. These are to be found in section 5(3) which excludes certain classes of document from the operation of the statutory provisions in section 5.

5.164 These include classes of documentary data and:

> "(a) information that is privileged from disclosure in criminal proceedings, (b) information supplied by a person who would not be compellable to give evidence at the instance of the party wishing to give the information in evidence by virtue of section 5 and (c) information compiled for the purposes of or in contemplation of (i) criminal investigation, (ii) investigation or enquiry carried out pursuant to or under any enactment, (iii) civil or criminal proceedings or (iv) proceedings of a disciplinary nature."[79]

5.165 The question of what qualifies as a business record when it comes to the process of admitting business documents in evidence focuses on the position of the documents within the overall administrative scheme of the enterprise. Business records are those documents which a business generates in the course of its activities and are not documents which are the product of that enterprise. This crucial distinction has been reaffirmed in Australian cases such as *Roach v Page*[80] and *ASIC v Rich.*[81]

5.166 An attempt to qualify a document as a business record will fail where the document in question is being drawn under the umbrella of a business record as a means to side-step the exclusionary rules and which are in practice incidental to the day to day operations of the business or have been generated with a view to litigation. Simply describing the documents as the side-effect of the core business activities where in reality they are the product of that business will not suffice. To be admissible in evidence a document must be an internal record maintained in the usual course of the business, recording business activities.

(b) Further Stipulations under the 1992 Act

5.167 The process of admitting evidence under section 5 of the 1992 Act also remains subject to the interests of justice in general. Section 8(1) of the 1992 states that:

---

79 *Criminal Evidence Act 1992* section 5 (3).

80 [2003] NSWSC 939.

81 [2005] NSWSC 417.

"in any criminal proceedings information or any part thereof that is admissible in evidence by virtue of section 5 shall not be admitted if the court is of the opinion that in the interests of justice the information or that part ought not to be admitted."

5.168 Section 8(2) lays down the following factors in determining whether the evidence is to be admitted in the interests of justice:

i) whether or not, having regard to the contents and source of the information and the circumstances in which it was compiled, it is a reasonable inference that the information is reliable,

ii) whether or not, having regard to the nature and source of the document containing the information and to any other circumstances that appear to the court to be relevant, it is a reasonable inference that the document is authentic, and

iii) any risk, having regard in particular to whether it is likely to be possible to controvert the information where the person who supplied it does not attend to give oral evidence in the proceedings, that its admission or exclusion will result in unfairness to the accused or, if there is more than one, to any of them.

5.169 Thus documentary evidence may be excluded where the court is satisfied it would be too onerous an obligation on the accused where the supplier of the information does not intend to give oral testimony during proceedings. The section places substantial emphasis on the evidential norms of admissibility and authentication, focusing on matters such as reliability,[82] authenticity,[83] and accuracy[84] in estimating the weight to be attached to a particular piece of documentary evidence.

5.170 The question of whether or not the evidence is admissible has little impact on the weight to be afforded to these documents. Determining the weight of the evidence is a function reserved to the arbitrator of fact and this is granted statutory recognition in section 8 as to any inferences which can reasonably be drawn as to the accuracy or otherwise of the proffered evidence under Part II *Criminal Evidence Act 1992*.

---

82 Section 8 (2)(a).

83 Section 8 (2)(b).

84 Section 8 (2)(c).

(4) Analogies between the Irish and English provisions

(a) Authenticating Electronic and Automated Documents as Admissible Evidence in England

5.171 In England the *Civil Evidence Act 1968* represented a concerted legislative attempt to address and overcome the strictures of the Hearsay Rule. While it did not abolish the hearsay rule it did introduce measures to allow for the admission into evidence of both oral and documentary hearsay in civil cases.

5.172 On the question of electronic evidence, the *Police and Criminal Evidence Act 1984* specifically regulated the collection of "computer evidence" and identified procedural processes which could be applied to electronic evidence with provisions dedicated to the means of gathering electronic evidence.

5.173 Certain provisions of the Irish *Criminal Evidence Act 1992* are broadly analogous to comparable measures in the English *Criminal Justice Act 1988*. For example section 5(3) of the *Criminal Evidence Act 1992* is broadly comparable to section 24 of the English 1988 Act.

5.174 The English courts have considered section 24 of the English 1988 Act and have held that before admitting a statement or document under the provision, the trial judge must have recourse to section 24(4) to assess the purpose for which the documents were made.

5.175 In *R v Bedi*[85] the defendants had been charged with offences connected with producing fraudulent sales vouchers and using both lost and stolen credit cards for this purpose. At their trial the prosecution had introduced documentary evidence of reports prepared by the bank relating to the credit cards. The banking documents had been prepared by bank employees at a central clearing section of the bank. On appeal it was held that the reports were business documents but the Court also held that the trial judge had failed to consider, under section 24(4) of the 1988 Act, the purpose for which the reports had been prepared. The Court of Appeal held that the motivation for which the documents were produced was not for the purpose of criminal proceedings but had arisen out of the conduct of the bank's business functions. This did not, therefore, attract the operation of the exclusions under section 24(4). The Court of Appeal also held that any question as to whether a document was prepared for the purposes of criminal proceedings or an investigation was a matter of fact and was be determined on a case-by-case basis by the trier of fact.

---

[85] (1992) 95 Cr App R 21.

5.176 Section 27 of the *Criminal Justice Act 1988* allowed for the admissibility of a copy of the document where the original was unavailable regardless of whether or not that document was still in existence. This copy would then be "authenticated in such manner as the court may approve" and it provided that there are no degrees of secondary evidence insomuch as "it is immaterial for the purposes of this subsection how many removes there are between a copy and the original." As amended by the *Criminal Justice Act 2003*, this now applies to "anything in which information of any description is recorded."[86]

5.177 An example of this can be seen in the English case *R v Leonard,*[87] concerning an appeal was taken following the admittance in evidence of unattributed text messages which had been extracted from a mobile telephone found in the defendant's possession. The substance of the text messages was the discussion of the quality of drugs and the text messages were admitted in support of charges for intent to supply drugs. The defence argued that the text messages were inadmissible hearsay. The judge rejected this argument but admitted them as evidence of the bad character of the accused rather than as hearsay, but admissible as falling within one of the exceptions and stopped short of classifying it as real or direct evidence. The Court of Appeal quashed the conviction and held that the texts were inadmissible as hearsay and should not have been offered to the jury. They amounted to "statements" under section 115(2) of the *Criminal Justice Act 2003* as "any representation of fact or opinion made by a person by whatever means; and it includes a representation made in a sketch, photofit or other pictorial form" and the purpose of which had been to cause the recipient to believe the matter stated therein or to act on the basis of this.[88]

5.178 Once it was established that the texts were hearsay the question then turned to whether they met the statutory requirements of admission. The only basis upon which they could be admitted was under section 114(1)(d). Under the provisions of section 114 this means that any such statement would be inadmissible as evidence of the matter stated unless drawn within one of the stated exceptions.

5.179 The court then turned to examine the intent of the statements contained in the texts. The issue was whether or not the defendant was a drug dealer and was not focused on whether the sender wished to make the recipient act on the information conveyed. On appeal the evidence was inadmissible

---

86 *Criminal Justice Act 2003* section 134 (1).

87 [2009] EWCA Crim 1251.

88 Section 115 (3).

hearsay for the purposes of the *Criminal Justice Act 2003*. Despite this there was still a very strong case against Leonard and the conviction was upheld as the initial admission of the texts had not tainted the rest of the trial.

5.180 When it comes to a relevant and admissible document, the position under English law is, therefore, that the Best Evidence Rule is no longer in issue. Where a statement in a document is admissible as evidence in criminal proceedings the information may be produced by the document or a copy of the whole or of the material part whether or not that document remains in existence. The statute leaves it to judicial discretion as to how best to authenticate the impugned document.

(5) Admitting Documentary Evidence Issues of Hearsay in South Africa

5.181 Section 34 of the South African *Civil Proceedings Evidence Act 1965* (CPEA) deals with admitting documentary evidence in civil proceedings. It provides that, where direct oral evidence of a fact would be admissible, any statement made by a person in a document which tends to establish that fact shall be admissible subject to certain conditions. While this generally necessitates the production of the original document this requirement may be relaxed under the provisions of section 34(2)(b).

5.182 In its application to electronic and automated documentary evidence, it was held in *Narlis v South African Bank of Athens*[89] that section 34 did not apply to computer output because it had not been generated by a person. Following this decision, computer output is now governed by the *Computer Evidence Act 1983* (CEA).

5.183 This means that in civil proceedings a computer printout is admissible where certain conditions are satisfied. The CEA not only lays down the mechanisms by which computer output may be authenticated, but also involves a general exception to the Rule against Hearsay where its provisions are observed.

5.184 Where the yield of a technological device has been sufficiently authenticated in terms of the CEA, which is done by means of filing an affidavit, it is admissible as evidence of any fact recorded therein of which direct oral evidence would be admissible under section 3 of the CEA (direct oral evidence would be admissible in any situation where the Rule against Hearsay might apply). Once the output information has passed these admittance hurdles and been authenticated, the evidential weight attached is determined by the court as it deems appropriate under section 4(2).

---

89 1976 (2) SA 573, AD.

5.185 In 1987 the South African Law Commission was of the view that for "the present the Commission is not convinced of an immediate need for a general investigation into the effectiveness of section 57 of the *Computer Evidence Act 1983*.[90] In 1995, when examined from the perspective of electronic evidence, the South African Law Commission recommended the repeal of the 1965 Act.[91]

5.186 Running parallel to the statutory mechanisms for authenticating electronic documentary evidence and the mechanisms associated with computer output in section 2 of the CEA, which deals specifically with authentication by means of affidavit, are the traditional common law means by which to determine to admissibility of a document which demand that any hearsay element to the output be brought within a recognised exception to the exclusionary rule. As the CPEA is confined to those statements made by a person, it would not be appropriate for the inherently mechanical element of much digital documentary evidence. However, the *Law of Evidence Amendment Act 1988* (LEAA) also relaxed the Rule against Hearsay. This operates in conjunction with the CPEA and in its application to civil and criminal cases it is not hindered in its operation by the requirement that the maker be a person.

5.187 In 2001 the South African Law Commission again addressed the area of electronic evidence in connection with computer crime.[92] In order for hearsay evidence to be presented under this regime, the information must first satisfy one of three requirements - that admission of the evidence has been agreed, that the person upon whose input the computer data relies has been called as a witness, and that the court can be persuaded that the evidence ought to be admitted in the interests of justice.[93]

5.188 New legislation governing this area was introduced in the *Electronic Communications and Transactions Act 2002,* which repealed the *Computer Evidence Act 1983*. Section 15 of the 2002 Act is based on Article 9 of the UNCITRAL Model Law on Electronic Commerce and also removed the Best Evidence Rule from South African law.

---

90 South African Law Commission (Project 6: Review of the Law of Evidence) Report 1987.

91 South African Law Commission, Project 95 Investigation into the Computer Evidence Act 57 of 1983, Working Paper 60, 1995.

92 Project 108 *Computer Related Crime: Opinions for Reform in Respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications related to Procedural Aspects*, South African Law Commission 2001.

93 *Law of Evidence Amendment Act*, section 3(1)(a),(b) and (c).

(6) Authenticating Electronic and Automated Documents as Admissible Evidence in Victoria, Australia

5.189 Section 55B of the *Evidence Act 1958* represented the first generation of evidence legislation through which to regulate the admissibility of electronic documentary records in Victoria. It constituted an exception to the Hearsay Rule, and records were only deemed to be admissible where they had been produced by the ordinary operation and use of the machine which had been regularly supplied to it with information (again not having been generated in anticipation of litigation) and at such time as the computer was functioning correctly. Section 55B (4) allowed the introduction of such records with a certificate from a suitable person as a means to verify them. Admissibility in such circumstances was based on the regularity and predictability of computer usage over the course of trade during which the computer was used regularly to store or process information. Other requirements related to the class of information contained in the record which had to have been regularly supplied to the computer over the period during which the record was generated and that, for the duration of the period in question, the computer was operating properly.

5.190 Section 55B incorporated routine automated documents and provided for their admissibility so as to prevent what would otherwise be the application of the Hearsay Rule. Crucially, the supply of the information could be by human intervention, in which case it was directed to the supply of data rather than more complex information".

5.191 This was the conclusion reached in 2003 in a review conducted by the Public Records Office of Victoria, which noted that section 55B would not allow the admission of a letter to prove its contents just because it was typed on a computer. "It will however, mean that valuable records demonstrating system authenticity or lack thereof, such as audit logs, are likely to be admitted without difficulty."[94]

5.192 The Victorian *Evidence Act 2008* is the means by which the uniform *Evidence Act 1995* has been integrated into the Victorian law of evidence. The rules of evidence are now bound by the provisions of the Victorian *Evidence Act 2008* which simplifies and modernises the key issues which impact on documentary evidence - the areas of "documents" as the units of proof for evidence and also resolves the notion of the original as being the best evidence and also addresses the ever-expanding area of electronic and automated documentary evidence. The *Evidence Act 2008* abolishes the Best Evidence Rule in Victoria which is specified in section 51. Other provisions now make

---

[94] Electronic Records as Evidence, Public Records Public Record Office Victoria, Advice to Victorian Agencies, PROA 03/08, Version 1, 1 May 2003, p 6.

allowance for secondary evidence to be admitted in the form of copies where offered in evidence.[95]

5.193 The *Evidence Act 2008* also incorporates electronic and automated documentary evidence as one which:

> "has been produced, or purports to have been produced, by a device that reproduces the contents of documents."[96]

5.194 This provision provides that electronic documents and records can be produced before the court in legible fashion which includes by means of a transcript where the primary "document" under discussion is for example a sound recording.[97] This means that relevant evidence cannot be excluded as inadmissible on the basis of form alone. Nor does the *Evidence Act 2008* impose any specific authentication criteria or strict foundation criteria for electronic records over their hard-copy counterparts. There is no attempt to introduce restrictive criteria based on the operation of the computer or mechanical device.

(7) Authenticating Electronic and Automated Documents as Admissible Evidence in the US

(a) The Existing Rules and Case Law

5.195 The United States has two important cases which delve into the issue of electronically stored information (ESI) as evidence - *Lorraine*, *US v Safavian*[98] and *In Re Vee Vihnee*.[99] The matter of a foundation element and the necessity of such a measure was discussed by Grimm J in *Lorraine v Markel American Ins. Co.*[100] The Court noted here that:

> "considering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted."[101]

---

95 *Evidence Act 2008* section 47 (1) (a) and (b).

96 Section 47 (1) (b) (ii).

97 Section 47 (1) (c).

98 435 F Supp 2d (DDC 2006).

99 336 BR 437 9th Cir BAP (Cal) 2005.

100 241, FRD 534 (D Md 2007).

101 241, FRD 534 (D Md 2007) at 538.

5.196 Judge Grimm's cautionary comment seems to recommend that evidential matters surrounding electronically stored information need to be examined at an earlier stage in proceedings at the authentication stage which in the case of ESI also would have implications for the discovery process.

5.197 Although issues surrounding admissibility and authentication arise in the main in the United States at the summary judgment stage,[102] Grimm J in *Lorraine* suggested that unsworn and thus unauthenticated documents would not be received in a motion for summary judgment as the Court is permitted to consider only that evidence which would be admissible at trial.[103]

(b) Authentication Electronic Documentary Evidence- Tools Available under Federal Rules of Evidence 104, 901 and 902

5.198 The main authenticating tools in use in the United States evidential regime are governed by two similar but equally distinct federal provisions. These are the "preliminary rulings" provision on admissibility, governed by Rules 104(a) and (b), and the Rules governing the determination of authentication - Rules 901 and 902.

5.199 As was made clear from Grimm's judgment in *Lorraine*, it is the function of the court rather than the task of the fact finder to make a determination on the admissibility of evidence. In undertaking this task the court is not bound by the traditional restrictions of the Rules of Evidence other than those which concern privileges.[104]

---

102 *Celotex Corp v Catrett* 477 US 317, 322, 106 SC 2548, 2552 (1986).

103 Grimm also laid down the differing evidential principles involved in this area describing the amalgamated rules as those which:

"...present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible." He laid down a series of evidential rules to be followed and observed where ESI is offered as evidence. These related to distinct Rules in the Federal Rules and included situations where the ESI has the potential to make some fact that is of consequence to the litigation more or less probable than it otherwise would be (in other words is it relevant?). Where it is deemed relevant is it authentic and can it be shown to be so? Is the ESI hearsay and if so does it fall within one of the exception categories? Is it an original or duplicate under the Best Evidence Rule or is there admissible secondary evidence to prove its content? Finally and crucially does the probative value of the ESI outweigh its prejudicial value?

104 Rule 104(a) governs the admissibility of matters such as whether an expert is qualified and, if that is the case, whether his or her opinions are admissible;

5.200 Yet the authenticity and therefore the legitimacy of electronically stored information as well as other evidence is governed by Rule 104(b), which assigns a more limited role to the court. The function of the court in such matters is confined to addressing a foundation threshold question of whether the evidence maintains sufficient probative weight which could sustain a finding that the evidence is in fact what the proponent claims it to be. It is in turn, the function of the fact finder to determine whether the evidence is authentic. Where for example an e-mail is offered into evidence in the US, the determination of whether it is authentic would be for the jury to decide under 104(b), and the facts that they consider in making that determination must be admissible evidence.

5.201 The tools used to actually authenticate the electronically stored information as evidence are to be found within the provisions in Rules 901 and 902. As is the case with real evidence, a party seeking to admit an electronic document must pass over the barrier of authentication and show that the evidence is indeed what he purports it to be.

(i) Authentication and the Role of Rule 901

5.202 Rule 901(a) of the Federal Rules of Evidence states:

> "(t)he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

5.203 Rule 901(b) offers, "by way of illustration only", examples of authentication or identification that conform with the requirements of Rule 901. With particular reference to computer records and documentation, Rule 901(b)(9) states that "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result" is required to authenticate evidence. The Advisory Committee for the Federal Rules of Evidence has noted that this rule can be applied to computer records, telephone records, voice identification processes, ancient documents or data compilations.[105]

5.204 Many courts have not required specific authentication procedures under 901(b)(9) for business records which have been merely stored on a computer. In these instances courts have required a higher foundation for authentication under 901(b)(9) when the computer system or process has been

---

existence of privilege; and whether evidence is hearsay, and, if so, if any recognised exception applies.

105 See further Advisory Committee's Note to Federal Rules of Evidence 901(b)(9) and www.federalevidence.com.

used as a means to produce electronic analysis specifically for the purposes of litigation. Because of this Rule 901(b)(9) is often not considered by courts when the issue is merely the introduction of computer printouts of business records.

5.205 The ease with which this can be accomplished has been judicially noted. In *United States v Safavian*,[106] which concerned the admissibility of emails, a Federal District Court noted:

> "[t]he question for the court under Rule 901 is whether the proponent of the evidence has 'offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is....' The Court need not find that the evidence is necessarily what the proponent claims, only that there is sufficient evidence that the jury ultimately might do so."[107]

5.206 While case law has discussed whether the authentication of electronically stored information may be deserving of greater scrutiny than that applied to the authentication of "hard copy" documents, US courts have not abandoned the traditional exclusionary approach. In *In Re Vee Vinhnee*[108] the 9th Circuit Bankruptcy Appeals Panel focused on the authentication of electronically stored business records. It noted that "[a]uthenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained."

5.207 The Court also noted that a paperless, electronic record presents more "complicated variations" on the authentication problem than paper records. The court did acknowledge, however, that, whatever the form the document might take, "it all boils down to the same question of assurance that the record is what it purports to be."[109]

(8) Reform

5.208 The arguments against imposing a separate evidential regime with a higher foundation requirement vastly outweigh any arguments promoting such a scheme. To resolve evidential matters relating to these records by reference to prescriptive criteria would create enormous expense and would involve a considerable time lag leading to delays in proceedings. It is also suggested that the benefits of such a scheme (greater certainty as to the authenticity of the electronic document dependent on establishing the reliability of the device

---

106 435 F Supp 36 (DDC 2006).

107 *Ibid,* at 38.

108 336 BR 437 (9th Cir. BAP (Cal)) 2005.

109 *Ibid,* at 444.

creating it) could not be guaranteed to the extent required to justify the onerous preconditions to be satisfied.

5.209 At the moment, a party offering electronic or automated documentary evidence can have this evidence admitted (where relevant) even though strictly, it should not be admitted for instance where it transgresses the rule against remote or documentary hearsay. The evidence is admitted because of a willingness to address the given document pragmatically and to include it by reference to one of the myriad exceptions and arguments which bend to the balance of convenience and see evidence admitted where drawn within categories of business records, bankers' books or public documents. There is also the possibility that a given document may be admitted having been drawn within a catch all exception. This is exemplified by United States cases such as *Palmer v AH Robins Co. Inc.* where the Colorado Supreme Court permitted computer records to be admitted in evidence as an exception under the common law "general hearsay exception". This saw records admitted where the information was pertinent to the proceedings and sufficiently reliable to be admitted in evidence.[110]

5.210 The Commission has made recommendations in connection with business records as an exception to the hearsay rule.[111] Admissibility would remain subject to the long-relied on provisos that the records be made at or near the time of the matters recorded by or from information transmitted by, a person with knowledge made pursuant to a regular practice of the business activity, kept in the course of regularly conducted business activity and where source, method, or circumstances of preparation must not indicate lack of trustworthiness.

E The Authentication and Recognition of Public Documents for Evidentiary Purposes

(a) The Authentication of Public Documents in Ireland

5.211 Authentication is the process by which documentary and other physical evidence is shown to be genuine, and not a forgery, and that it has been written or attested to by the party claiming to have done so. Generally, authentication can be established in one of three ways.

5.212 Firstly, a witness can testify as to the chain of custody through which the evidence passed from the time of its generation until the trial. Second, the evidence can be authenticated by the opinion of an expert witness examining

---

110 684 P .2d 187, 202 (Colo. 1984).

111 See above paragraph 4.09.

the evidence to determine whether it has all of the properties that would be expected of an authentic document. Thirdly, authentication can arise, in effect, from the operation of a combination of common law or statutory presumptions of due execution or exceptions to the best evidence rule.[112]

5.213 At common law there is a presumption of due execution and attestation of certain documents and that they were generated on the date on which it was purported to have so been.[113] This presumption is raised once the document has been in existence for 30 years or more and comes from the proper custody channels that is, that it has been kept in a place with which it would be logically associated.[114] Furthermore, strict proof of due execution will not be required where notice has been served on the party in possession of the document to produce it and where they have refused to do so. In essence they should not benefit from any attempt to obstruct the legal process.[115]

5.214 As the Commission has already discussed,[116] at common law there exists a wide exception to the hearsay rule when it comes to admitting public documents as prima facie proof of the facts contained in them. The basis for this is rooted the expectation that such documents have been recorded dispassionately and that the relevant registrars or compilers can be taken "to perform their duties honestly and conscientiously"[117] particularly where the documents are liable to public scrutiny.

5.215 This exception was extended at common law to admit secondary evidence of the contents of public documents in deference to both the practical and financial difficulties inherent in the production of originals.[118] These documents will usually be *prima facie* admissible and do not require further authenticating testimony. The standard will be met by simply showing that they are printed by official government printers and bear the stamp, seal or signature of particular officers or departments.[119] McGrath also notes that the maxim

---

112 McGrath, *Evidence*, Thomson Round Hall, 2005, p 688.

113 *Anderson v Weston* (1840) 6 Bing NC 296.

114 *Doe d Jacobs v Phillips* (1845) 8 QB 158; *Thompson v Bennett* (1872) 22 UCCP 393.

115 *Jones v Jones* (1841) 9 M&W 75.

116 See Chapter 3.

117 McGrath, *Evidence*, Thomson Round Hall, 2005, p 259.

118 *Mortimer v M'Callan* (1840) 6 M & W 58 at 68.

119 *People (DPP) v McCormack* [1984] IR 177.

omnia praesumuntur rite et solemniter esse act[120] applies and raises a rebuttable presumption that a public document has been properly executed once an admissible copy is adduced.

5.216 In the context of the conveyancing of land, section 59(1) of the *Land and Conveyancing Law Reform Act 2009* provides that "[r]ecitals, statements and descriptions of facts, matters and parties contained in instruments, statutory provisions or statutory declarations 15 years old at the date of the contract are, unless and except so far as they are proved to be inaccurate, sufficient evidence of the truth of such facts, matters and parties." This 15 year rule replaced a 20 rule in section 2(2) of the *Vendor and Purchaser Act 1874*.

(2) Documents Originating From or Intended for Use in Another Jurisdiction

5.217 In an increasingly global economy, public documents are often needed outside the State in which they originated. As we have seen, there is an evidential presumption within a State that such documents have been duly authenticated, although this presumption may not apply outside the State. The Commission notes, however, that by virtue of the State's membership of the European Union, comparable presumptions apply to, for example, the text of Directives published in the Official Journal of the European Communities.[121] Indeed, it has been pointed out, like their national counterparts, since EU public documents "derive from an objective source and represent a reliable and durable source of information [this] makes them the most appropriate means of evidence for proving EC rights.[122]

(a) Proof of public documents under the 1961 Hague Apostille Convention

5.218 The principal function of a public document is to record factual proof of the acts of a public authority recorded therein and which are of interest to the public. They are admitted as the case law demonstrates as evidence subject to the proof of their authenticity and certification. Public documents enjoy presumed authenticity and are extremely relevant when attempting to resolve any mutual assistance enquiries. However while many foreign public documents enjoy a privileged evidential value some member states require these documents to be authenticated and naturalised through legalisation.

---

120 "All acts are presumed to have been done rightly and regularly." McGrath, *Evidence*, Thomson Round Hall, 2005, p 689.

121 See above paragraph 3.71

122 British Institute of International and Comparative Law, Study JLS/C4/2005/04, *The Use of Public Documents in the EU*, July 2007.

5.219 Outside the EU setting, however, Irish law does not apply a presumption that, for example, an adoption order made by a public authority in another State is proof either that the document has been made (real evidence) or that it is proof of its contents (by way of an inclusionary exception to the hearsay rule that, for example, a child had been abandoned and was eligible for adoption in that other State).[123] In these international settings, the 1961 *Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents* sets out a process for the recognition of foreign public documents through a verifying document called an Apostille.[124]

5.220 The background to the 1961 Convention is that, before certain documents can be used outside their originating State, prior authentication of the document may be necessary. This is often the case where overseas officials are not able to determine the authenticity of a document. When a document is destined for use in a foreign country, this authorisation is often accomplished through a public notary.[125]

(b) The role of public notaries

5.221 A notary is a public officer whose role is to serve the public in non-contentious matters usually concerned with foreign or international business. At a basic level the role of this officer (in Ireland, often also a solicitor) is to prevent fraud by attesting that the person identified as having signed a document did in fact sign it. The signature and official seal of a notary suffices as evidence as to the authenticity of a writing, which allows documents to be recognised internationally.[126] Notaries are appointed by the Chief Justice and their seals are retained by the Registrar of the Supreme Court.[127] Prior to appointment a

---

123 See, for example, *Dowse v An Bord Uchtala* [2006] IEHC 64; [2006] 2 IR 507, discussed in the Commission's *Report on Aspects of Intercountry Adoption* (LRC 89-2008).

124 *See Report on the Hague Convention abolishing the requirement of Legalisation for Foreign Public Documents* (LRC 48-1995) in which the Commission recommended ratification of the 1961 Convention.

125 On the use of notaries in Ireland, see generally, www.publicnotary.ie

126 The duty of a notary is to the transaction as a whole rather than to just one of the parties. A Notary may act for both parties to a transaction as long as there is no conflict between them and his duty is to ensure that the transaction they conclude is fair to both sides.

127 Section 10(1)(b) of the *Courts (Supplemental Provisions) Act 1961*, replacing section 19(3) of the *Courts of Justice Act 1924.* See *Re McCarthy* [1990] ILRM 84.

prospective applicant must pass a test set by the Examination Body of the Faculty of Notaries Public in Ireland.[128]

5.222 In Ireland, the notary's signature and seal are certified by the Department of Foreign Affairs. The notarised and embossed document is then produced at the Consular Section of the Department of Foreign Affairs in Dublin where the signature of the Registrar of the Supreme Court is in turn verified. The final part of the procedure sees the document produced to the consular representative in Dublin of the foreign country in which it is sought to be produced where the Irish Consular Officer's signature is recognised and legalised.

5.223 Notarial authentication is common in documents relating to transactions of a commercial nature, and so it is not necessarily confined to public documents. In instances of private documents the authentication in question will be the seal of a public notary appended to the private document to certify the physical fact of the execution of the document or the signature in a notary's presence. Notarial authentication is also used for legal and public documents to establish their authentication or verify an aspect of their execution in the process towards authorisation. Proof of authentication in this way means establishing that all formalities to enable the document in question to be accepted by judicial authorities as admissible evidence have been complied with.

(c) Specific requirements of the 1961 Hague Apostille Convention

5.224 The 1961 Hague Convention sets out the formalities for "legalising" public documents for recognition outside the originating State by means of a pre-printed form called an Apostille. In this context, the word "apostille" derives from the French word for certification. Public documents in this context include materials relating to the transfer of ownership of property, adoption orders and registrable contracts. The purpose of the 1961 Convention is to simplify procedures for recognition of such documents, thus bypassing the need for a continuous chain of verification signatures and seals in order to render the document effective in the country in which it is produced.

5.225 It also removes previous requirements for diplomatic or consular legalisation for public documents originating in one Convention country and intended for use in another. Indeed, consular officers in Convention countries are prohibited from placing a certification over the Convention Apostille.

---

[128] See the Practice Direction of the Chief Justice, 28 March 1994, and Order 127 of the *Rules of the Superior Courts 1986,* inserted by the *Rules of the Superior Courts (No. 2) 1993* (SI No. 265 of 1993).

5.226 The Apostille is formatted in numbered fields that allow data to be understood by the receiving country regardless of the official language of the issuing country. An attached Apostille entitles the document to recognition in the country of intended use, and no further authentication or legalisation by the embassy or consulate of the foreign country where the document is to be used is required.

5.227 The legalisation procedure entails a series of "consecutive verifications each of which constitutes a link in an unbroken evidential chain from which the authenticity of the document can be concluded."[129] The overriding purpose of legalising and apostillising documents is the prevention of fraud. These apostillised documents are entitled to recognition in any other Convention country without any further authentication and other States which are parties to the Convention are obliged to extend this recognition. A fully completed Apostille certificate confirms the person that signed the document has the authority to do so. It is a means of harmonising procedures to ensure that the document should be recognised without further authenticating evidence prior to use in another state which is party to the Hague Convention 1961.

5.228 Under the Convention, "public document" means documents emanating from an authority or an official connected with the courts or tribunals of the State, including those originating from a public prosecutor, a clerk of a court or a process-server ("huissier de justice"), administrative documents, notarial acts and official certificates which are placed on documents signed by persons in their private capacity. An example of this would be an official certificate recording the registration of a document, such as a birth certificate, or the fact that it was in existence on a certain date or official and notarial authentications of signatures.[130] The main provisions of the Convention are as follows:

> "Article 2. Each Contracting State shall exempt from legalisation documents to which the present Convention applies and which have to be produced in its territory. For the purposes of the present Convention, legalisation means only the formality by which the diplomatic or consular agents of the country in which the document has to be produced certify the authenticity of the signature, the capacity in which the person signing the document has acted and, where appropriate, the identity of the seal or stamp which it bears.
>
> Article 3. The only formality that may be required in order to certify the authenticity of the signature, the capacity in which the person

---

129 Functions of a Notary Public available at www.notarypublic.ie.

130 Article 1, 1961 Hague Convention.

signing the document has acted and, where appropriate, the identity of the seal or stamp which it bears, is the addition of the certificate described in Article 4, issued by the competent authority of the State from which the document emanates.

Article 5. The certificate shall be issued at the request of the person who has signed the document or of any bearer.

When properly filled in, it will certify the authenticity of the signature, the capacity in which the person signing the document has acted and, where appropriate, the identity of the seal or stamp which the document bears. The signature, seal and stamp on the certificate are exempt from all certification.

Article 8. When a treaty, convention or agreement between two or more Contracting States contains provisions which subject the certification of a signature, seal or stamp to certain formalities, the present Convention will only override such provisions if those formalities are more rigorous than the formality referred to in Articles 3 and 4."

5.229 The formalities themselves leave open the possibility of deception and are arguably vulnerable to fraud given the loose association of signatures and the impossibility of comparison with an unavailable original. The formalities are dependent on the mutual trust and administrative cooperation of Member States for the operation of the Apostille system. The system is dependent upon the recognition by each State of the measures of the others to ensure the authenticity of their public documents.

(3) Irish legislation implementing the 1961 Hague Apostille Convention

5.230 Ireland ratified the 1961 Hague Convention in 1999. Since then, a number of legislative provisions have been put in place to allow for recognition of foreign documents authenticated under the Convention. The *Rules of the Superior Courts (Proof of Foreign, Diplomatic, Consular and Public Documents) 1999*[131] set out the relevant rules of court concerning the recognition of public documents which have been authenticated under the Convention, without the need for legalisation. Section 6 of the *Investment Funds, Companies and Miscellaneous Provisions Act 2006* provides for the authentication of business documents internationally under the 1961 Convention.

5.231 Most recently, section 3A of the *Statutory Declarations Act 1938*, inserted by section 50 of the *Civil Law (Miscellaneous Provisions) Act 2008*,

131 S.I. No 3 of 1999.

provides for an extremely wide-ranging power to make statutory declarations abroad in accordance with the 1961 Convention. Prior to the changes made by the 2008 Act, the *Statutory Declarations Act 1938* required a declarant to make the declaration before an Irish diplomatic or consular office in an Irish embassy or consular mission. While this means of making such a declaration will continue, section 3A of the 1938 Act, as inserted by the 2008 Act, provides for making such declarations using the Apostille process of the 1961 Convention. This was done in recognition of the difficulties encountered by persons as result of the restrictive nature of the original regime in the 1938 Act. The alternatives now available include making a statutory declaration before a person qualified under section 1 of the 1938 Act, namely, a notary public, a commissioner for oaths, a peace commissioner or a person authorised by law to take and receive statutory declarations. Section 3A of the 1938 Act also makes it possible to use whatever the local equivalent process may be to the solemn form of making a statutory declaration as it exists under Irish law, including the Apostille method. The changes made by the 2008 Act were modeled on section 6 of the *Investment Funds, Companies and Miscellaneous Provisions Act 2006*.

(4) Authenticating Documents for use in Countries Not Party to the Hague Convention 1961

5.232 The law does allow for some degree of differential treatment as between foreign and domestic public documents provided that this is proportionate given the objective differences between the documents. Whether permitted or not it must be borne in mind that member states usually rely on the mutual trust principle when presented with a public document from a fellow nation State that has been duly executed by the authorities of that State. If the country where the documents are to be used is not a signatory to the Hague Convention 1961, these documents will need to be legalised by a Notary Public. After an Apostille has been issued by the Department of Foreign and sent to the consul of the relevant foreign embassy the consul then adds their own certificate. Where a country is not party to the Convention, “legalisation” must be carried out by the diplomatic or consular mission of the country in which the document is to be used and it is left to the discretion of the foreign mission to choose what standards and processes to apply to decide whether a document is authentic.

(a) Legalisation of documents in States not party to the 1961 Hague Apostille Convention

5.233 If the country where the documents are to be used is not a signatory to the 1961 Hague Convention, these documents will need to be “legalised,” that is, formally authenticated. The process of “legalisation” must be carried out by the diplomatic or consular mission of the country in which the document is to

be used, and it is left to the discretion of the foreign mission to choose what standards and processes to apply to decide whether a document is authentic. This more formal process is clearly less satisfactory than the standard form Apostille provided for by the 1961 Convention.

(b) The Position of a Notary Public with Regard to Authenticating Foreign Language Documents

5.234 Notarisation is the attestation by a Notary Public that the signature appearing on the document is true and genuine. This is a formality usually completed in the State where the document originates. Notarisation may be a prelude to "legalisation" and once notarised a document may need to be apostillised if it is to be used extra-jurisdicitonally.

5.235 Notorial authentication of a document may be necessary as the 1961 Hague Convention specifically adopted the definition of a public document to include notorial acts.[132]

(c) Apostille and notarial processes do not verify contents of documents for evidential purposes

5.236 The Commission emphasises, for the purposes of this Consultation Paper, that neither the notarial nor the Apostille process serve to verify the document involved as to the proof of its contents. The notary's role is limited to attesting to the certification on the document. The notary must satisfy himself or herself that the person producing the document understands the document. Following this the document is stamped with a statement to the effect that "[t]he notarial act is limited to the verification of the identity, legal capacity, name and signature of the Appearer, unless otherwise expressly stated in the English Language."[133]

(d) Challenges posed to notaries by Electronic Documents

5.237 It is clear that documentary authentication has long existed through the process of notarisation. Fully automated devices, independently producing information captured in documentary form represent a difficulty for evidential concepts which are traditionally dependent on interactions involving human input. Questions arise as to how traditional notarisation techniques can be adopted to apportion and establish responsibility to transactions which are concluded by an autonomous electronic matrix rather than by human parties. This development requires new means of authentication to supplement the traditional notarisation mechanisms associated with the physical world where a person furnishes the notary with proof of his or her identity and residence. The

---

132 Hague Convention 1961 Article 1 (c).

133 See further www.notarypublic.ie.

Commission notes here that the use of electronic signatures involves an attempt to introduce a comparable method of verification of identity for an electronically derived document. The Commission returns to discuss this possible solution later in the Consultation Paper.[134]

5.238 In the context of digital records, much of the focus is on the ease with which they can be altered or destroyed as well as the difficulty of establishing with any degree of certainty that such a change has taken place.

5.239 Computer documents are easier and cheaper to generate, maintain and reproduce requiring little or no exertion to copy and distribute when compared with their paper equivalents. Since these digital documents take up virtually no space, little effort is needed to destroy them when they are no longer needed. While it may be thought that an electronic document can be easily deleted, it is in fact virtually impossible to expunge the information entirely. At the very least, a reconstructible shadow of the document from a computer hard drive can be reconstructed. The traditional concept of deletion is really an exercise in freeing up and recycling space as the computer memory will merely tag the space previously taken up by the now recycled document as being available space. While it may not be readily visible the information persists in the electronic matrix and can be retrieved.

5.240 In a further distinction with paper documents, many active files on computers, especially shared data on network servers, are in a constant state of flux and are subject to being edited, added to, subtracted from, or deleted. Although there is a dearth of empirical evidence to suggest that electronic documents are more frequently altered, the Commission acknowledges that they are prone to manipulation in ways that paper files could never be.

5.241 Section 30 of the *Criminal Evidence Act 1992* provides for the admission of copies "whether or not the document is still in existence by producing a copy of the document or of the material part of it authenticated in such manner as the Court may approve."[135] Section 30(2) of the 1992 Act provides that it is irrelevant how many degrees separate the copy from the original, nor is the admissibility prejudiced by the means of reproduction.

5.242 In effect section 30 of the 1992 Act permits the prosecution to rely upon material contained in copy form, provided that the Court is satisfied, as a condition precedent, that the information is admissible in evidence. This is a hugely important provision as it means that where the authenticity of the copy documents can be established to the satisfaction of the court, any true replica of documentation can be adduced regardless of form. The Commission notes

---

134 See Chapter 7.

135 *Criminal Evidence Act 1992* section 30 (1).

here, as it has done previously in the Consultation Paper, that the 1992 Act obviously applies in criminal proceedings only and no comparable provision has been enacted for the purposes of civil proceedings.

5.243 *The Commission provisionally recommends that notarised documents should be admissible in civil proceedings on conditions comparable to those in section 30 of the Criminal Evidence Act 1992.*

CHAPTER 6 AUTHENTICATING SPECIFIC FORMS OF ELECTRONIC AND AUTOMATED EVIDENCE

6.01 In this Chapter the Commission takes the discussions in Chapter 5 on questions of how to authenticate documentary evidence and how to establish the integrity and reliability of a piece of documentary evidence and applies this to different forms of electronic and automated evidence. In doing so Part A examines how to establish the chain of custody of an electronic document (which may go through several drafts and which are often in continual flux; gaining additions or losing material and passing through several different computer banks during this process). It also addresses the different strains of electronic documents which may emerge from a single initial device for example video and audio recordings and the subtle but distinct differences between analogue and digital photographs and how these are to be authenticated. The Commission discusses how to establish the provenance of the documents emanating from these devices for the purposes of evidence.

6.02 Part B examines how different electronic documents can be brought before the courts and what questions arise surrounding their admissibility and authenticity. This includes a discussion on telephone records as admissible evidence and whether this is real evidence or documentary hearsay. It also discusses the admissibility of secondary documentary evidence such as transcripts of recordings and translations and the purpose for which they are received (for example to support oral expert testimony or as a procedural tool against witness intimidation). Also investigated are the questions surrounding automated documentary evidence and the authentication of mutable computer evidence.

6.03 Part C examines the process by which electronic and automated documentary evidence can be brought before the courts. In this respect the Commission looks at the procedural aspects of the discovery process with particular reference to electronic documents and questions of record management and destruction, following which it may be necessary to re-generate or create new documents if needed in evidence. Part C examines the costs and burdens involved in blanket disclosure of voluminous electronic documents and how to streamline the process through initiatives which permit the presentation of electronic evidence electronically.

6.04 Part D briefly looks at the means of regulating electronic documents in a commercial setting and the legislative provisions which have been introduced in the area, as well as the regulation of electronic devices such as internet communications and domain names.

A The Application of Evidential Norms to Differing Strains of Documentary Evidence.

(1) Chain of Custody

6.05 The point of creation, or indeed the individual creator of the document may be in issue for evidential purposes and that person may be unidentifiable. The Commission now turns to address the means by which the documents may be stored in differing systems and the evidential issues that arise from this.

(a) Electronic Documents

6.06 If a digital medium like a disk or a hard drive contains evidence which is disputed, the only way that this will be admissible in litigation is if a "chain of custody" is proven. It must also be proven that the evidence was not altered in any way, in particular in the analysis stage of evidence like a computerised log-file, that the data could be inadvertently manipulated. Evidence can also be accidentally damaged in transporting it from one area to another. It can also happen that a piece of digital code is altered when a machine in going through its "power-down" cycle and will purposely destroy any designated files or wipe a disk drive by means of a virus.

6.07 Decisions in the United States have indicated points of convergence occurring between mechanically generated documents and their paper-based counterparts. The decisions in *In Re Vee Vinhnee*[1] and *Lorraine v Markel American Ins. Co.*[2] touched on the hurdles encountered in attempting to balance and resolve these issues.

6.08 Analogies can easily be drawn with the traditional, default regime of paper-based, tangible evidence when addressing the concerns which mechanically and electronically generated records give rise to.

6.09 The mechanics of creating and storing paper-based tangible records and the systems that maintain these largely stable records are generally simple and easily understood. The element of control over such data hinges on physical access to the records, and therefore any alteration or manipulation

---

1 336 BR 437 (9th Cir. 2005).

2 241, FRD 534 (D Md 2007).

done by another party would be detectable and traceable by following the chain of those physically controlling the custody of the information.

6.10 Thus any attempt to manipulate or destroy (either fully or partially) the document can be easily detected through an examination of, for example, indentations, missing fragments or frayed edging. This is only possible, however, where the control system has been designed to reflect the physical realities of the environment in which the records are maintained.

(2) Video and Audio Recordings

6.11 There is a significant difference between video recordings and electronic digital image reproductions. Video recordings are usually admitted as real evidence. Where a copy is derived from a tape recording, the copy may be of a lesser quality than the original and further derivative copies if made from a copy may mean that the results are degraded and ultimately unusable. Reproducing an electronic image however, consists of a series of binary digits which can be copied an unlimited number of times without affecting the quality and with no degradation of the images as compared to the original. The derivatives are essentially indistinguishable from the original. Where the electronic document contains metadata, the metadata will have changed with each copy and the document will be identifiable as a derivative.

(3) Analog and Digital Photographic Images

6.12 Photographs and digital photographic images may also have an identifiable history and may have passed along a chain of custody. For example, an image stored digitally may have been captured with a camera and the image then converted into digital format for transfer to another device or for storage and then converted back to analogue for display.

6.13 If a digital photographic image is altered, the fear that this could pass undetected is not sufficient to exclude these documents from evidence. If an image of this sort has been altered then the associated metadata will also have changed and will reveal the manipulation. This is in contrast to strictly physical photographs where manipulation may pass unnoticed as the only investigative tool is the human eye. This has been identified as legally problematic since the development of photography. In 1899, the American case *Cunningham v Fair Haven & Westville R. Co.* identified the issues as being that:

> "either through want of skill on the part of the artist, or inadequate instruments or materials, or through intentional and skilful manipulation, a photograph may not only be inaccurate but dangerously misleading."[3]

---

[3] 72 Conn. 244 at 250, 43 A. 1047 at 1049.

6.14 Image distortion has, therefore, been on the legal radar for quite some time and the Commission therefore considers that electronic imaging does not really create new legal problems. Rather it provides another technology for potential distortion, but it is also notable that, at the same time, it also provides the means by which to detect the extent of any fraudulent manipulation.

(4) Intentional, Detectable Distortions

6.15 Many decisions in the United States have identified the inherent difficulties with such digital documentary materials. To overcome such difficulties courts in the US undertake a preliminary hearing to determine the admissibility of the documents.

6.16 For example, in *State of Washington v Hayden*[4] the defendant's trial for murder involved evidence produced by computer enhancement of fingerprint images. Fingerprints were found at the scene of the murder but in their raw state were too subtle to identify. Enhancement techniques were used to filter out the background environmental and bacterial patterns and colours of the sheet, and the latent prints were identified and as those of the defendant. A preliminary hearing on the scientific evidence (a Kelly-Frye hearing[5]) was undertaken where the defence objected on the grounds that the digital images introduced had been manipulated. The court authorised the use of digital imaging and the defendant was found guilty. The defendant's appeal against conviction was dismissed.

6.17 This case followed *State of Virginia v Knight*[6] which was the first case to accept electronically enhanced images as admissible evidence. It involved an enhanced secondary image of a bloody fingerprint found at the scene. A Kelly-Frye hearing was held to determine the scientific validity and acceptance of the enhancement process. The court was of the opinion that the techniques were essentially photographic processes and that the image was admissible.

---

4 1998 Wn App (1st Div) 25.

5 The Frye standard is broadly speaking the mean acceptance of evidence when discussed from a scientific/legal perspective. It has been subject to "critical analysis, limitation and finally outright rejection" in favour of the Daubert test for analysing digital forensic evidence or documentary images. See Heesing and Sangin, *Digital Evidence Collection Procedure in Digital Forensics and the Admissibility of Digital Evidence*, available at www.kic.re.kr/english/research/ebook.

6 (1991) CR-90-1353-02-F.

6.18 In *State of California v Jackson*[7] the defendant had appealed a death sentence on several grounds, one of which concerned a Kelly-Frye hearing, but the court ruled this unnecessary as the digital processing technique had become a readily accepted practice in forensics and new information was not added to the image during the process any more than the use of a microscope would have added to material it magnified.

(5) Establishing the Provenance of Electronic Images

6.19 The ease with which digital images can be copied and retransmitted would appear to favour a cautious approach when seeking to admit electronic images as evidence. While a court is likely to admit the evidence it is prudent to remember that the judge will direct the jury on the weight they should consider attaching to it. Establishing the provenance of the document remains an issue and the person adducing a recording as evidence must describe its provenance and history so as to satisfy the judge that there is a prima facie case that the evidence is authentic. The evidential weight of the electronic document will be informed by authentication methods such as encryption or watermarking. This could also be accomplished by undertaking an audit trail connecting the initial image with the computer record which is to be adduced in evidence and which documents the shifts in the image.

6.20 Situations such as these do not arise in the case of electronically stored or generated materials where access to the information, other than that guarded by electronic signatures and password encryption is not naturally constrained to such a high degree.

6.21 With the modern inter-locking and inter-relating functionality of computer networks and systems in which most computers participate as members, if not in unison then in sync, the means by which to maintain a sufficient degree of control and security has become an area which is often out-sourced or delegated to persons who are fully competent in information and computer technology.

B The Application of Evidential Norms to Differing Strains of Documentary Evidence.

(1) Telephone Records

(a) Admitting Telephone Records in Ireland in Criminal Proceedings

6.22 The data located and recorded in mobile telephone records may be of enormous evidential value. This data can be stored on the mobile telephone handset, inserted memory cards and on the SIM card. Particulars of every

[7] (1995) No. SCD 105476.

telephone call made are automatically recorded by the Service Provider with details taken as to the name of the subscriber, the time at which the call was placed, whether the call was connected or answered, the identity of the telephone number to whom that telephone call is made.

6.23 These steps combine to form a process called "connection charting exercises" and involve forensically examining the history of incoming and outgoing calls. Other particulars recorded include the location of the handsets involved with the areas of coverage and divided into cells from which the telephone call is made. This information is extrapolated by reference to the nearest local base station[8] and the duration of the call and is known as cell site analysis whereby each call connection is coordinated by geographical cell.[9] This is not to say that the forensic examination of a mobile telephone does not have its limitations in that only a partial view of past connections and time accuracy may be constructed. For instance multiple calls may not be recorded. Although cell patterns shift and cell behaviour as to strength and integrity may change even within a room the pattern matching which is undertaken may be indicative of call behaviour and builds a picture of the circumstances surrounding an incident.

6.24 The electronic footprint left by mobile telephones has become an effective investigative tool and the ubiquity of the handset has been likened to a "personal electronic tagging and tracking device"[10] pinpointing the location of a given mobile phone with ever increasing certainty.

6.25 The admissibility of telephone records arose in *The People (DPP) v Prunty*[11] where the principle in the UK *Myers* case was applied by the Court of Criminal Appeal. The defendant had been charged with a number of offences including false imprisonment. Part of the prosecution case was based on telephone calls relating to the payment of a ransom. The prosecution contended that the defendant's voice was identified from recordings made and the process of tracing those calls was also admitted as evidence. The defendant contended

---

8 Each cell has a unique number associated with it and the number is recorded by an automated system for each connection.

9 Cell site analysis is a technique used to determine what cells a mobile telephone is likely to connect to given the behaviour of the mobile network at particular geographical points/regions of interest. This information is then related to the call data records provided by the mobile networks to determine possible locations of a mobile telephone at the time of past connections. Lecture on Forensic Evidence by Keith Borer Consultants.

10 Kelleher, "*Privacy and Data Protection law in Ireland*", Dublin, Tottel, 2006, p 401.

11 [1986] ILRM 716.

that the process of tracing and producing these exhibits should be excluded as hearsay evidence. The trial judge ruled that the evidence was admissible.

6.26 The Court of Criminal Appeal upheld the appeal and ordered a re-trial. It was alleged that the means by which to establish the sequence of proof was baseless having offended the rule against hearsay. The Court held that the evidence in the case as to tracing involved an element of hearsay in the chain of proof and was thus inadmissible in the absence of any verifying witness testimony. The Court however indicated that had an essential witness been unavailable it might have considered the information as being admissible but that this was not so and therefore the documents were inadmissible. McCarthy J stated that:

> "It may be as in *Myers* case, where the essential witness cannot be obtained, the Court should feel obliged to admit records, albeit hearsay, but there is no evidence that such is the case here. At first sight, in any event, it would seem that a means of proof analogous to that of the *Bankers Books Evidence Act* would require the intervention of the legislature".[12]

6.27 It is notable, of course, that since the decision in the *Prunty* case the case the Oireachtas has, indeed, intervened to enact the *Criminal Evidence Act 1992,* the equivalent of the *Bankers Book Evidence Acts* for the purposes of criminal proceedings.

6.28 Qualitative difficulties also arise with electronic data. These recordings and demonstrative documents may contain garbled signals and poor sound quality. The Court in *Prunty* discussed, but in effect dismissed, these difficulties as issues which would rule the electronic evidence inadmissible. The Court of Criminal Appeal stated that in proceedings where mechanical evidence forms the lion's share of the evidence and consists of a tape recording, and where this tape is shown to be authentic, defects in audio quality as well as disputes as to the identity of the speakers are not sufficient to render the evidence inadmissible. Such ambiguities were for the trier of fact to resolve. In addition, despite the possibility that there were potentially more persons available to give evidence as to the identity of the speakers, this was not a sufficient ground for excluding the recording from evidence although the trial judge should always direct the jury as to sound quality of evidence and any effects this may have on its weight.

6.29 In this respect, the Court also held that any defect in the quality of the electronic documentary evidence was not a matter of admissibility but rather went to the weight to be attached to it. In *Prunty* the identification of the

---

12 [1986] ILRM 716 at 718.

defendant had been undertaken by a detective Garda, although the Court noted that he had not been acting in his public, but rather his persona, capacity: he had been a childhood acquaintance of the defendant and therefore his knowledge of his speaking voice on the telephone was very limited and had not been tested within the previous 12 months.

6.30 The Commission considers that the approach taken in the *Prunty* case is apt for inclusion in the proposed statutory framework, and that this would be applicable in both civil and criminal proceedings. The Commission has therefore provisionally concluded that, in the case of mechanically recorded electronic documentary evidence, if it is shown to be an authentic recording, any defects in the quality of such a recording or a dispute as to the identity of the speaker on the recording will not be a ground for ruling it inadmissible in evidence. The Commission also provisionally recommends that any such issues should go to the weight of the evidence rather than to admissibility.

6.31 The Commission provisionally recommends that, in the case of mechanically recorded electronic documentary evidence, if it is shown to be an authentic recording, any defects in the quality of such a recording or a dispute as to the identity of the speaker on the recording will not be a ground for ruling it inadmissible in evidence. The Commission also provisionally recommends that any such issues should go to the weight of the evidence rather than to admissibility.

(i) Mobile Telephone Records as Real Documentary Evidence in Criminal Proceedings

6.32 Mobile telephone data is compiled automatically by the telephone operator's computer system. As such it is deemed to have been generated digitally and is classed as automated "real" evidence for the purposes of litigation. Where the compilation of these records involves human input, it will suffice for such a document to be proved by the certificate process of the *Criminal Evidence Act 1992*.

6.33 In *The People (DPP) v Murphy*[13] the defendant was alleged to have given two mobile telephones to another person to assist him to move explosives to Northern Ireland for a bombing operation the day before the explosion occurred. The prosecution sought to admit telephone records showing that these phones had been used in the vicinity of the bombing on the day of the explosion. The defendant submitted that these were inadmissible as hearsay. The Court of Criminal Appeal held that the fact that the telephone records had been produced mechanically without human intervention did not render them inadmissible as hearsay. Instead they were admissible as real evidence, and

[13] [2005] IECCA 1; [2005] 2 IR 125.

this applied not merely where the evidence was produced by a device which processed information supplied to it, but also where the device itself gathered information. The Court also held however that in order to have the records admitted it was necessary to call evidence to describe the function and operation of the computer. The Court also held that the *Interception of Postal Packets and Telecommunication Messages (Regulation) Act 1993*, which prescribes the circumstances in which telephone communications may be traced, contained sufficient safeguards so as not to contravene the defendant rights under the Constitution or his right to privacy Article 8 of the European Convention on Human Rights.

6.34 Similarly, in *The People (DPP) v Meehan*,[14] the Court of Criminal Appeal also held that, in respect of a phone log, a wholly automated mechanical process was involved when, following the transmission of the application form under the 1993 Act, the registration of the name and number had taken place and once allocated had been entered on the company's computer. It was this process which had resulted in the printout of the documentation to which the defendant objected. The appeal, however, did not centre on the accuracy of the automated recording or billing system.

6.35 Instead the defendant contended that the documentary statements did not satisfy the provisions of section 5 of the *Criminal Evidence Act 1992* and were not admissible. The defendant contended that, apart from the 1992 Act, the evidence was not admissible under common law rules of evidence. In the alternative, counsel submitted that the records relating to the identity of the subscriber did not satisfy the common law principles for the admission of records generated mechanically and were not acceptable in evidence.

6.36 The Court of Criminal Appeal rejected the argument that section 5 of the *Criminal Evidence Act 1992* had the effect of excluding evidence of this nature unless it complied with the provisions of the Act. Were such an approach to be endorsed it would have the effect that any common law rules as to admissibility of documents in criminal proceedings would thereby have been abolished. The Court approved, in this respect, the comments in *The People (DPP) v McCann*[15] where Carney J stated:

> "[Counsel's] point as regards time in relation to s.7 of the *Criminal Evidence Act 1992* would be unanswerable were the State proceeding by certificate under s.5 of the *Criminal Evidence Act 1992*. They are not, in fact, doing that, but are proceeding under the pre-existing procedures prior to the *Criminal Evidence Act 1992*…

---

14 [2006] IECCA 104.

15 Central Criminal Court, 31 July, 1996.

one should consider the entirety of the *Criminal Evidence Act of 1992* as a whole and it provides a mechanism of proof of certain matters by certificate. But even then it provides that in certain circumstances proof shall nevertheless proceed in the traditional and pre-existing fashion by oral evidence. I am satisfied that the *Criminal Evidence Act 1992* provides ample alternatives to pre-existing procedures but does not abolish them."[16]

6.37 The prosecution relied on a range of circumstantial evidence which it was argued was far too tenuous to ground a prosecution. As noted above this included mobile telephone records and CCTV footage, stills and analysis and evidence of e-mail footage. Taken cumulatively this kind of circumstantial evidence can, in the words of the current Director of Public Prosecutions, combine to provide for a "logical inference of guilt when the inculpatory facts are incapable of any other reasonable explanation".[17]

6.38 Documentary evidence from mobile phone service providers was also an element in the subsequent case of *People (DPP) v O'Reilly*[18] where mobile phone triangulation techniques were used to locate Mr. O'Reilly's phone. The case arose when the applicant sought to appeal the conviction for his wife's murder. There were several issues on which the appellant sought appeal including grounds relating to tracking and electronic evidence. The applicant challenged the admissibility of several parts of the evidence at the trial and in particular, but not exclusively, the evidence relating to the phone records and documents admitted to show the phone's usage pattern.[19] It was also argued

---

16 At the trial in *People (DPP) v McCann* questions were also advanced as to the right to privacy a person can expect in relation to his telephone records set against the conflicting Garda duty to investigate crime and examine all material evidence including that of phone records. The resolution of these issues depended on whether or not the evidence regarding telephone records should be properly excluded. With the conclusion that there was sufficient unchallenged oral evidence of the existence of a licence and that therefore the Gardaí were entitled to obtain the telephone records pursuant to their statutory powers, it was not necessary to consider the arguments relating to privacy over the documents.

17 Hamilton, "From CSI to Court: Electronic Communications and the Prosecution of Crime", Law Society Annual Criminal Law Conference, 15 November 2008, p 1.

18 [2009] IECCA 18.

19 There were various grounds of appeal including that the trial judge had erred in permitting the prosecution to adduce evidence of interviews with the applicant in custody where it was clear that he had exercised his right to silence and that the trial judge had erred in refusing to exclude from the jury a witness statement in

that it had not been proven that O2 Ireland was a licensed operator within the meaning of section 7 of the *Postal and Telecommunications Services (Amendment) Act 1999* and that the judge should not have admitted the mobile phone records.

6.39 It was also contended that the evidence of an individual analysing the movements of a motor vehicle by CCTV should have been excluded and further that the trial judge had refused to exclude prejudicial emails. All avenues of the appeal were refused. Murray CJ found in particular that the emails were manifestly admissible and relevant evidence and that the passage of time was not so considerable. They were sufficiently proximate to the crime to be material evidence.

6.40 In *The People (DPP) v Kavanagh*[20] the Court of Criminal Appeal again acknowledged that telephone evidence can be an important part of a prosecution case. The nature of both fixed landlines and mobile telephones were considered. The characteristics of a landline and its limited mobility were noted as was the flexibility of a mobile phone which has the facility to be registered to a particular user or have its use assigned to a particular individual by following the connections of the cells used to transmit these calls which are routed to the nearest available mast. The Court accepted that "such evidence is admissible and it may be highly probative"[21] as had been established in *The People (DPP) v Meehan*.[22]

6.41 The telephone evidence in question related to calls placed to the deceased's mobile telephone which had ceased transmitting at a particular time. This time became relevant to approximating the time of death and was evidence of the deceased's profligate use of his mobile telephone during his lifetime. The telephone records were admissible as evidence to establish a pattern of use and it might have reasonably been expected that he would have recharged it. Instead the phone had ceased to function. Evidence was also adduced, to indicate the mast through which mobile telephone calls were routed by the deceased and the appellant. In dismissing the appeal the court was of the opinion that there was no legal difficulty in relation to the telephone evidence adduced in the present case. This evidence was clearly admissible and relevant.

---

circumstances where the applicant was a suspect and had no caution administered to him. The Court of Criminal Appeal dismissed all grounds.

20 [2009] IECCA 29.

21 *Ibid*, at p 4.

22 [2006] 3 IR 468.

6.42 These cases illustrate that the traditional principles of evidence are being used to admit digital evidence without reference to form and without the need on the part of the courts to introduce new foundation criteria to establish authenticity. Electronic and automated evidence is being taken as sufficiently authentic and admissible so that whatever issues are associated with this evidence does not affect its admissibility based on form alone.

(2) The Admissibility of Audio and Visual Recordings and Transcripts

(a) Application of the principles extended by Butera to Electronic Audio and Video Evidence in Ireland

6.43 A transcript is a documentary record setting out the information contained on an electronic medium. As such it is the production in permanent legible form of the documented information conveyed electronically. It does not constitute a copy of the tape for example but is rather a copy of what can be heard on the tape. The Australian case *Butera v DPP*[23] which has been discussed already[24] noted that "the rule excluding secondary evidence did not go beyond writing and included physical objects."[25] At present there is no legislative presumption that a translation is an accurate translation for evidential purposes.

6.44 In this respect, Irish law has adopted an inclusionary approach[26] to video evidence so as to extend and adapt its definitions to comply with the Best Evidence Rule rather than having to accommodate it via an exception, as demonstrated in recent case law.

6.45 A similar approach has been taken in other States to determining the admissibility of a photograph or a tape recording.[27] The traditional view is that graphics and video and audio footage constitute real evidence rather than strict documentary evidence subject to the exclusionary rules. Real evidence need only be relevant and meaningful to be admitted. This is determined by the court following the interpretation of expert opinion and judicial discretion to admit or exclude evidence.

---

23 *Butera v DPP* (1987) 164 CLR 180.

24 See paragraph 2.69-2.75 above.

25 Dixon J in *Commission for Railways (NSW) v Young* (1962) 106 CLR 535 at 544.

26 *Criminal Evidence Act 1992* and *Offences Against the State (Amendment) Act 1972*.

27 *R v Ali* [1966] 1 QB 688 at 701 and *Butera v DPP* (Vict) (1987) 164 CLR 180 at 192.

(b) Electronic and Automated Documentary Evidence Admitted to Provide Greater Clarity to the Court

6.46 *In re Wards of Court* and *In Re MK, SK and WK, Minors: The Eastern Health Board v MK and Another*[28] focused on the admissibility of hearsay evidence. The disputed electronic evidence in this case was a tape recording of interviews with the young complainants. While the debate focused on whether such devices were more properly described as "hearsay evidence", Keane J was of the opinion that in regard to video evidence generally, far from breaching the hearsay rule:

> "there may be cases where a tape recording, once established as being authentic, may be the best evidence of the happening of a particular event."[29]

6.47 Keane J discussed the niche into which electronic and automated documentary evidence fell and how best the law of evidence could or should accommodate it. He noted that electronic evidence could be seen as an evolved type of evidence providing real insight and categorical evidence, building a clear picture of what occurred for presentation to the court. In doing so he discussed how:

> "a tape recording may give an extremely accurate picture of how an accident happened. Likewise a tape recording may give a more accurate picture of a burglar than a witness who merely had a fleeting glance at him in a moment of crisis. Even in the case of reported speech a tape recording may be more accurate than hearsay because it can give us the exact words which the person whose speech is recorded used and also the demeanour of that person at the time when he used them."[30]

6.48 Keane J thus indicated he supported the admission of such data and placed it at least on a par with, if not superior to oral testimony in such circumstances.

(c) Electronic and Automated Documentary Evidence Admitted to Support Export Opinion Testimony as Source Material

6.49 When discussing expert evidence, Keane J also referred to the use of electronic devices (again tape recordings) and examined the decision in

---

28 [1999] 2 ILRM 321.

29 *Ibid*, p 9.

30 *Ibid*.

State (D&D) v Groarke.[31] Although it was peripheral, an issue arose as to the admissibility of video recordings to support claims by a medical doctor of sexual abuse in relation to the child at the centre of the case. Here Finlay CJ held that in order to determine whether the conclusion reached by the doctor who had interviewed the child was sound, the court should properly have had access to the basic evidence from which such conclusion was reached (ie the video tapes).[32]

6.50 The tape recordings in *Groarke* were viewed as a tool upon which the social worker based his opinion and therefore should have been available in evidence as material which would have supported his testimony. In such circumstances it is then for the trier of fact to accept or reject that evidence.

6.51 The undoubted probative value of audio evidence was also highlighted in *Fyffes Plc v DCC Plc*[33] The plaintiff company sought a declaratory order that certain share sales involving the defendant were unlawful dealings within the meaning of Part V of the *Companies Act 1990*. In relation to audio evidence, recordings from tapes had been offered in evidence. The High Court appeared to express a latent distrust of transcript evidence of the tapes offered in evidence. It was noted that:

> "the transcripts of the tapes should be approached with caution and that in-depth scrutiny of particular words and phrases used in the course of telephone conversations can be apt to mislead."[34]

6.52 On the other hand the recordings were acceptable as offering an insight into what transpired, not only during the course of the telephone calls but also recorded other information and "shed light on what went on before and in the intervals between the calls."[35]

6.53 In *Southern Health Board v CH*[36] the issue was whether a video recording of an interview between a child aged six and a half and a senior social worker was admissible into evidence. O'Flaherty J emphasised the best interests of the child. The focus was not on creating a further exception to the hearsay rule. Instead what was in issue was how expert evidence should be

---

31 [1990] 1 IR 305.

32 Ultimately, the admissibility of hearsay evidence was not raised and instead the court looked to the expert evidence of the medical doctor.

33 High Court, 21 December 2005.

34 *Ibid*, p 156.

35 *Ibid.*

36 [1996] 1 IR 219.

approached. He held that the documentary video evidence was admissible as that of the expert. This was because as well as the expert's opinion evidence, O'Flaherty J felt that the source documentary materials upon which the opinion was based should be before the Court. In this regard the tapes constituted admissible material to back up the expert testimony.

(3) Electronic and Automated Documentary Evidence Admitted as a Procedural Tool

6.54 The concern for the Irish courts following these cases is how to take the principles forward and adapt them to cases other than those of vulnerable child witnesses and other vulnerable witnesses in cases of abuse and to make electronic evidence admissible as stand-alone real evidence. The statements by the child in *SHB v CH* were admitted in limited circumstances. They were not admitted as to the truth of what was said. They were admitted as having been said, but only to be used as source material for the opinion of an expert.[37]

6.55 Video evidence is increasingly coming before the courts where it is tendered as and accepted as real evidence. In determining the admissibility of the documentary footage judicial discretion will be exercised and consideration given to the applicability of any exclusionary rules of evidence. The recording must be authentic, and of sufficient quality and probative value before being admitted in evidence. When determining whether to admit video evidence it is the relevance, and quality which, along with judicial discretion will determine admissibility.

6.56 Video evidence can provide a useful procedural tool against intimidation. The admissibility of a video recording of testimonial statements as evidence has been on a statutory footing since the enactment of the *Criminal Evidence Act 1992*[38] and the *Criminal Justice Act 1999*.[39] Section 39 of the *Criminal Justice Act 1999* provided a mechanism by which witnesses who would be vulnerable to intimidation may give evidence via recorded television link where the District Judge is satisfied that the witness is likely to suffer fear or intimidation arising from giving evidence.[40] This is admissible in evidence in

---

37 It is likely that the weight the Court would attach to expert opinion based upon such source material will be less than that given to such opinion when the expert has conducted the interview and had it recorded on video.

38 Part III, section 16.

39 Section 39.

40 This also extends to pre-trial procedure where either the accused party or the DPP may apply to the trial court for an order requiring a witness to appear before the District Court for the purposes of giving evidence by means of deposition, or where there is a risk of intimidation, by means of recorded video link.

various circumstances including where the witness does not offer oral testimony at the trial of the action owing to intimidation. The video evidence is subject to restriction and there must have been an opportunity to cross-examine the witness before the District Judge and the accused.[41]

6.57 In 2007 the Court of Criminal Appeal confirmed in *DPP v Larkin*[42] that it is now established that video footage is admissible as documentary evidence during the course of a criminal trial as evidence and a tool to identify an alleged offender. This case also confirmed the earlier case of *DPP v Foley*[43] which clearly stated that evidence from a still photograph taken from a video recording or the video recording itself is admissible evidence in criminal proceedings. But there were limits placed on this powerful evidential tool by the court which stated that the evidence might not be admissible where its probative weight was outweighed by the prejudicial impact of the document.

(a) Judicial Acceptance of Recording Devices and Transcripts as Admissible Documentary Evidence in the US

6.58 The need for an accurate means of dispassionately recording and retaining information was recognised over 100 years ago in *Rajnowski v Detroit*[44] where the Supreme Court of Michigan acknowledged the unsatisfactory state of affairs especially as regarded questions of interpretation because when immediate translation takes place:

> "the conflict of testimony is such as to indicate either more perjury than seems possible, or more likely incorrect renderings of testimony.
>
> It is necessary to employ the help of those who are supposed to understand both languages, and to be capable of transmitting correctly from each to the other all that is said by either person dealing with another.
>
> If stenographers could take down what is said by interpreters and witnesses in other languages, it might furnish some help, by giving means of resorting to other translators to test their accuracy; but this is also impracticable, and the stenographer's minutes contain the questions in English, and the interpreter's English rendering of the

41 *Criminal Justice Act 1999*, section 4F (3) (a).

42 [2008] IECCA 138.

43 [2007] 2 IR 486.

44 (1889) BC & AR Co. 41 NW 849.

answers, with no means of judging the correct report of either, as between interpreter and witness."[45]

(b) The Status of these Devices as Documents in England

6.59 In England, questions on the status of audio recordings and their relative position as documentary evidence has been discussed in cases like *Grant v Southwestern and County Properties Ltd*[46] as to whether a tape recording of a telephone conversation could rightly be counted as an admissible document. This case came for adjudication after *Beneficial Finance Corporation Co. Ltd v Conway*,[47] where McInerney J had held that this style of recording information was not a document. He based this finding on the assumption that while an audio tape recording documents recorded information and serves a function corresponding to that of a document, it is not a document because the information is not capable of being visually inspected. It was therefore the reproduction of the information in permanent legible form upon which this adjudication foundered.

6.60 However in *Grant* Walton J would not accept the conclusion that if two parties brought the same information to court; one by means of a tape recorder and the other handwritten, then only the written record would be discoverable and admissible in evidence. Furthermore, should the written document be in shorthand it would require some further translation or need a key to unlock the meaning which would add a layer of difficulty to it, a hurdle which the audio recording would not have to overcome. He stated that:

> "the mere interposition of necessity of an instrument for deciphering the information cannot make any difference in principle. A litigant who keeps all his documents in microdot form could not avoid discovery because in order to read the information extremely powerful microscopes or other sophisticated instruments would be required. Nor again, if he kept them by means of microfilm which could [not] be read without the aid of a projector."[48]

(i) The Status of these Devices as Documents in Australia

6.61 The High Court of Australia noted in *Butera v DPP*[49] that it is not the recordings themselves which comprise the evidence but instead it is that which

---

45 (1889) BC & AR Co. 41 NW 849 at 850.

46 [1975] Ch 185.

47 [1970] VR 321.

48 [1975] Ch 185 at 197.

49 (1987) 146 CLR at 180.

they record which is the evidence to be tendered. The Court must first be satisfied that the proposed visual recording evidence is relevant and that it does not breach any of the exclusionary rules of evidence. Where audio recordings are available or spoken words can be heard on tape-recordings, these will potentially breach the rule against hearsay and must qualify as an exception before admittance.

6.62 In *Butera* the Court queried the relationship between a tape-recording of a conversation in a foreign dialect and its correlation to the written English transcript. The question in issue was essentially which was the evidence? This is a conflict which Morris identified as the struggle between "ideal v practical arrangements".[50]

6.63 The Court concluded that a tape-recording was only admissible in evidence once it was played as it was the sounds captured therein rather than the physical tape itself which was the evidence. Once played, the transcript was deemed admissible where the court was satisfied that it was an accurate representation of the information. Yet it was not independent evidence of the conversation but was instead an aid to interpreting and understanding the contents of the tape. It was secondary evidence of the contents of the tape. By analogy the recording on a tape or other fixed documentary medium falls squarely within the definition of a document reproduced in permanent legible form.

6.64 The sound recording must crucially be authenticated before it is heard during proceedings. This may be achieved by accompanying witness testimony as to that witness's knowledge of the surrounding circumstances in which the sound recordings were generated or in regard to the integrity of the materials used in making the recording and its functionality[51] as well as attesting that the record has not been tampered with.

(c) Conclusion

6.65 A potential note of contention with regard to adducing a transcript and support for the contention that it remains an aid to interpretation and not a true copy has been identified by the New Zealand Law Commission.[52] Here it was recognised that a transcript could lead to a false impression of the

---

50 Morris, R. (1993) "*Images of the Interpreter: A Study of Language Switching in the Legal Process*", unpublished Ph.D. thesis, Lancaster University.

51 Section 146 of the *Uniform Evidence Acts* of Australia facilitates this.

52 New Zealand Law Commission, "Preliminary Paper, Evidence Law: Documentary Evidence and Judicial Notice", NZLC PP22, May 1994, at 63.

evidence devoid of the nuances and tone which the words may have carried in their oral and audio form.

(4) Automated Machine Evidence

6.66 The combined 1997 appeal cases in the House of Lords of *DPP v McKeown* and *DPP v Jones*[53] related to the reliability of the Lion Intoximeter 3000.[54] When the readings were taken the computer clock on the machine was noted to be displaying a time some hour and a quarter slower than it should have displayed. The time differential had not been a point of contention at the trial of either case and nor had it been disputed in either case.

6.67 The appeals arose jointly following the finding of the Divisional Court who held that the reliability of the machine had been compromised and that this nullified and tainted the convictions. The admissibility of these items of documentary evidence was noted to be a "specialised exception to the hearsay rule", an exception which permits documentary evidence to be admitted where the police officer would ordinarily be required to give oral testimony. Instead the evidence by certificate is admissible on mere production subject to certain safeguards that the certificate and statement be served on the accused.

6.68 Where notice is given and the prosecution are obliged to call the officer for oral testimony as to what he saw on the machine's display this is considered to be real evidence under the common law as was noted in *Castle v Cross*[55] citing the earlier case of *Statue of Liberty*.[56] However where the

---

53 [1997] 1 All ER 737.

54 The Lion Intoximeter 3000 consisted of a breath specimen analyser which measured the alcohol content of the breath by means of an electrical pulse whereupon a computer converted the signal into digital form displaying the result of the test in visual form. The machine was equipped with a printer and a breath simulator which provided air containing a measured quantity of alcohol so that the operator could determine whether it was calibrating correctly. The standard procedure was for the machine to be tested before and after the analysis of the two specimens provided by the motorist. For the purposes of the *Road Traffic Offenders Act 1988* the Lion Intoximeter was an approved device in line with section 7(1). Evidence of the proportion of alcohol in the breath was adduced in court by certificate under section 16 of the *Road Traffic Act 1988*. This was done by means of the production of a documentary statement automatically produced by the device and accompanied by a certificate signed by the police officer where the statement related to a specimen provided by the accused at the date and time shown in the statement.

55 [1984] 1 WLR 1372.

56 [1968] 1 WLR 739.

machine contained a computer component the evidence was admissible only to the extent that it satisfied the requirements of section 69 of the *Police and Criminal Evidence Act 1984.*[57] This section, required that before any evidence originating from a computer was admitted, it first had to be established that the computer was operating correctly and had not been used improperly.

6.69 In *DPP v McKeown* both specimens were deemed to have failed the test for maximum allowable alcohol content and the statement had been signed by the constable upon which the "time shown on (the) print out is 1 hour 13 mins slow". The respondent had been served with the statement as to the failed test and a further statement from a director of the laboratory who provided the police force with the machines to the effect that the breath analyser system was independent of the mechanisms and circuitry of the clock and the failure of the latter could have no effect on the former. He later gave oral testimony to this effect and the court accepted that the breath analysis by the Intoximeter was not affected by the clock and that the statements as to the breath readings it produced were accurate.

6.70 Prior to the prosecution the CPS informed the respondent's solicitors that the lab station technician would offer testimony but refused a request to produce diagrams or documents. It was not until the hearing of the case a year later that the defence applied for an order that the documents and diagrams should be produced. A question arose as to whether the CPS had a right to refuse the application for production of documents as "material evidence" under section 97(1) of the *Magistrate's Court Act 1980*.

6.71 The CPS did not attempt to lay foundation evidence for the machine by demonstrating how a circuit diagram operated so as to show that the clock did not affect the machine's breath analysis element. The Divisional Court did not take objection with this. At the time of the case, automated documentary evidence of this calibre, with its reading and analysis determined by the computer had to satisfy the requirements on the admissibility of a statement in a document produced by computer as evidence under section 69(1) of the *Police and Criminal Evidence Act 1984*. Admissibility under subsection (1)(b) was determined with regard to whether:

> "at all material times the computer was operating properly, or of not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents."

6.72 The Court were of the opinion that the computer was clearly not in proper working order and that the inaccuracy of the time reading affected the

---

[57] Repealed by section 60 of the *Youth Justice and Criminal Evidence Act 1999.*

accuracy of a part of the contents of the document. However, despite this the court did not apply such a literal meaning to section 69(1) and made an analogy between the time being misrepresented and a software fault which caused the document to be printed in lower case when it was meant to be in upper case. Lord Hoffman noted that in such a situation the:

> "fault has certainly affected the production of the document. But a rule which excluded an otherwise accurate document on this ground would be quite irrational."[58]

6.73 The Court went onto discuss the nature and applicability of section 69 which was concerned with the proper operation and functioning of a computer rather than with determining the veracity of the information fed to the computer. This was instead seen as a question of weight for the trier of fact. Section 69 was concerned with the manner in which the disputed machine had held or processed the information as a condition of the admissibility of the computer-generated statement. The conciliatory language of section 69(1) was such as to recognise that although a computer may in the strict sense be malfunctioning, this is not of itself relevant to the purpose of the exclusionary rules and it was not the case that any failure which did not relate to the task the computer was designed to carry out was sufficient to adversely affect the capacity of the computer to process information correctly.

6.74 The Court then attempted to adjudicate on the level of malfunction which would be sufficient to exclude the evidence as inadmissible. They decided that a:

> "malfunction is relevant if it affects the way in which the computer processes, stores or retrieves the information used to generate the statement tendered in evidence. Other malfunctions do not matter."[59]

6.75 In *DPP v Jones* the defendant had provided only one specimen of breath which registered as containing more than four times the allowable alcohol level. He was deemed to have failed to provide a second sample. The police officer conducting the breath analysis noted that the time display was inaccurate by an hour and 15 minutes. The defendant submitted that the only evidence that his second breath specimen was inadequate was the computer reading showing that the test had aborted. Were this evidence to be held disqualified and inadmissible for failure to comply with section 69(1) he could not be convicted. However, this line of reasoning had earlier failed in the *McKeown* case and was similarly defeated.

---

58 Judgment available at www.publications.parliament.uk.

59 Lord Hoffman.

(5) The Authentication and Admissibility of Mutable Computer Evidence

6.76 E-mail and other new forms of computer-mediated communication such as the World Wide Web, chat rooms, bulletin boards, and voice mail can present many problems when time comes to having them admitted for the purposes of litigation.

6.77 In the US the Sedona Conference marked out e-mails as requiring detailed attention at every level – "retention, preservation, collection, production, and metadata" owing to the evidentiary challenges presented by this medium and its presumed innate unreliability.

6.78 Email and WebPages may be susceptible to "spoofing", where the sender imprints the e-mail with the name of another individual thereby making the message appear to originate from a different location. This is often accomplished through the use of an alien computer.

6.79 In terms of the evidential issues surrounding these forms of communication there are many shared characteristics when it comes to authentication. While evidence originating from websites and that linked to text messaging have shared standards for authentication, documentary evidence of interaction and communication made through chat-rooms pose different problems. This stems from the anonymity so frequently displayed by and associated with the medium. This is so because chat room messages can be legitimately posted by third parties using "screen names," and aliases and therefore it cannot be assumed that the content was posted with the knowledge or authority of the website host.

6.80 Adducing either a single e-mail or a chain of e-mail traffic regardless of whether these are hard-copy printouts or latent electronic images retained in a database raises some different evidential issues but even these can be accommodated within traditional documentary evidence frameworks. In order to come within the consideration of a document for evidentiary purposes, the authenticity of the e-mail and the potential application of Best Evidence Rule must be considered. Difficulties in this regard centre on the authentication of the sender's identity and linking him with the contents of the communications.

6.81 While giving oral testimony may resolve any superficial issues, difficulties remain where there are two conflicting, contradictory oral testimonies and where for example the recipient produces an e-mail printout but the alleged author denies ever sending such a message or vice versa. In such a situation, regard must again be had of judicial discretion to refuse to admit the evidence. On the other hand sufficient evidence speaking to the authenticity of the document may be found in the document itself in the electronic signature attached. These electronic signatures are analogous to a written signature or

embossed symbol which has been affixed to a paper document. Another possibility for authenticating an e-mail is to identify the sender's metadata (this may be electronically woven into the header for example of an email) and which will usually accompany an e-mail and identify the sender, the date and the time.

6.82 Discovery of e-mail is synonymous with electronic discovery. The volume and character of e-mail make it a prime target for discovery for commercial litigation. Different types of word-processed documents or e-mail messages may become permanent once completed but data compilations such as WebPages and information data banks are dynamic and always in flux.

(6) Reform

6.83 Deletion of computer files often does not destroy the file, but merely marks the disk space the file occupies for overwriting if needed. Given the ever-expanding memory capacity of modern computers it is unlikely that a washed or deleted file could be systematically overwritten. Electronic or automated documentary evidence from computer networks also automatically generates a wealth of evidence on their own activities, in the form of "ghost data" which may include information about who had access to what data or equipment at any given time. This only adds to the complexity of discovering electronic evidence.

6.84 This systematic churning of data means that when a matter is referred to for litigation, the information system should and must be frozen in time to preserve the discoverable evidence. Creating a permanent backup of a file from the moment it becomes the subject of litigation is easy and inexpensive and may benefit from incorporation in statutory form.

6.85 Questions arise as to the admissibility of the contents of social networking sites. Such cases would currently labour under the established evidential principles. There are two significant admissibility issues which threaten to scupper any attempt to gather the evidence on social-networking sites such as MySpace and Facebook. These are concerns as to authentication and the evidentiary rules' prohibition on hearsay. A third admissibility issue that may be implicated with these situations is the Best Evidence Rule. In the United States, Rule 1001(3) of the Federal Rules of Evidence expressly address the issue by stating that "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" [60]

6.86 In any jurisdiction electronic records, whether originals or copies, which are produced via routine business processes are likely to be admissible. In such circumstances they will fall within the business records category, being

[60] Federal Rules of Evidence, Article X, Rule 1001 (3).

less prone to being challenged as false documents in comparison to documents produced for specific purposes, such as litigation.

6.87 Reform proposals could involve requiring that parties prove the integrity of a document and show that it has not been tampered with. It can be said that the current arrangements of external third party accreditation takes the process of proving the integrity of the documents away from the supervision of the court. Instead, a system could be introduced based on the ability to demonstrate who has interacted with the records, and in what manner, to the satisfaction of the court. Techniques which could be employed in this respect include the use of audit logs to show who accessed, altered or updated records, when, and to what extent. Information could be required detailing whether adequate security measures have been employed in the maintenance and generation of the data records. This would accompany digital signatures and other authentication technologies to form a comprehensive means of establishing the lineage and integrity of the documents.

C Bringing Electronic Documentary Evidence Before the Courts; Discovery of Electronic Records

6.88 The Commission now briefly turn to discuss the means by which documentary evidence comes before the court. This will focus in particular on electronic documentary evidence which is a more challenging form of evidence and whose e-characteristics poses problems for discovery. These e-documents may have been deleted but are discoverable and can be reconstituted. Questions are raised as to who bears the costs of the search and reconstitution of what may often be voluminous documents and which is a task that is both time consuming and expensive.

6.89 Documentary discovery is a widely adhered to norm in Irish civil proceedings, ordinarily occurring on close of formal pleadings. Such discovery is in general not automatic and it must be requested by one of the parties (the judge cannot order discovery *ex-officio*). Non-party discovery can also be obtained either voluntarily or by order of the court whereby the party who seeks discovery must satisfy the court that the discovery is "necessary for disposing fairly of the cause or matter or for saving costs"[61]. This is executed by the issuance of an anton pillar order to preserve the data and prevent potentially sensitive information being lost through deliberate destruction.

---

[61] Order 31 Rule 12 of the *Rules of the Superior Courts* as substituted by *S.I. No. 233 of 1999* in relation to High Court proceedings. The test under Order 32 Rule 1 of the *Circuit Court Rules 2001* in relation to Circuit Court proceedings is less onerous. However, in practice, requests for discovery in Circuit Court proceedings usually meet the requirements of the High Court test.

6.90 The extent of the phrase "necessary for disposing fairly of the cause or matter or for saving costs" was considered by Kelly LJ in the Northern Ireland case *Lanigan v Chief Constable,*[62] in which he examined statements which, in his view, were potentially of significance in establishing precisely what "necessity" means in this context. Of potential aid in interpreting such a provision was whether:

> "[The statements sought are] very likely to contain material which would give substantial support to [the plaintiff's] contentions? Would he be deprived of the means of proper presentation of his case?[63]
>
> [Can it be said] there [is] a likelihood that the documents would support the case of the party seeking discovery? [Is there] something beyond speculation, some concrete ground for belief which takes the case beyond a mere 'fishing' expedition?"[64]

6.91 The party seeking discovery of the documents must meet certain standards and is required to specify the precise class of documents in respect of which discovery is sought and must set out reasons for each category,[65] particularly in cases of non-party discovery[66] the Courts retain a discretion not to award non-party discovery. This is exercised where it considers such an order would unduly oppress or prejudice the non-party.[67]

(1) Discovering Electronic Documentary Evidence

6.92 Issues arise in regard to the discovery of electronic and automated documentary evidence. Problems surrounding these documents relate primarily to their discovery. In 1985 a US district judge noted that:

> "(c)omputers have become so commonplace that most court battles now involve discovery of computer-stored information".[68]

---

62 [1991] NI 42, 52.

63 Lord Fraser in *Air Canada v Secretary of State for Trade* [1983] 2 AC 394.

64 Lord Wilberforce in *Air Canada.*

65 Rules of the Superior Courts (No 2) Discovery, 1999.

66 The onus lies on the party seeking discovery to establish that the party named is likely to have the documents in his possession, custody or power, and that they are the documents which are relevant to an issue arising or likely to arise in the matter in accordance with Finlay CJ in *Allied Irish Banks plc v Ernst and Whinney* [1993] 1 IR 375.

67 *Ulster Bank Limited v Byrne,* High Court, O'Donovan J, 10 July 1997.

68 *Bills v Kennecott Corp*. 108 FRD 459, 462 (D. Utah 1985).

6.93 There are also issues where a party has been served with notice to produce a document within the confines of his profession and fails to do so. The opposing party may then admit secondary evidence as proof of the document.[69]

6.94 The unusually large volume of electronic documents which may be collected even routinely or coincidentally over the course of a business or commercial transaction means that full discovery would involve the introduction of huge volumes of documents including draft material. The repetition involved as well as the pace at which electronic devices operate to produce electronic data and documents in which to record this information militates against any accurate discovery of data on a voluminous scale.[70] This level of physical discovery could have the effect of submerging the proceedings in unnecessary documentation. While the law of hearsay may operate to exclude voluminous presentation of documents on the basis of relevance, problems may occur where cases involve excessive hard-copy evidence which touches the proceedings. This may result from a deliberate attempt to scupper the court process or from innocent over diligence.

6.95 One means of ensuring the discovery of relevant documents to the exclusion of irrelevant or fragmentary evidence in the public sphere is to encourage the introduction of e-government structures and accept the electronic issuance and filling of documents by a public body as having been correctly executed as admissible evidence where required.

(2) Electronic Discovery

6.96 Order 31 Rule 12 of the Rules of the Superior Courts 1986, as amended in 1999, provided for the discovery of "electronically stored information" also referred to as ESI. Electronic and automated documentary evidence had previously been subject to undiluted civil law discovery provisions. Oder 31 traditionally saw hard-copy documents discovered where relevant to proceedings. The modernisation of the Rules brought electronic documents squarely within the remit of the courts. The danger remained that courts would be reluctant to extend traditional principles to novel categories of electronic or

---

69 *AG v Kyle* [1933] IR 15.

70 Further problems have been suggested such as those asserted by Whitfield, Gurney and Witfield, "*Databases Can Be Riddled With Errors; In Litigation, Computer Evidence Open to Challenge*", Legal Times, February 11, 1991, American Lawyer Newspapers Group Inc. to the effect that such data imputers need not even be literate as well as highlighting the problem that such tasks may have been subcontracted even to different jurisdictions where there is no scope to adequately monitor or set standards and where there may be different languages or methods employed or subject to homophonic errors.

automated evidence. This was made clear by the Supreme Court decision in *Dome v Telecom Eireann.*[71]

6.97 The discovery of specific electronic documents for admittance in evidence has not then posed a challenge for the Irish courts and *Clifford v Minister for Justice*[72] cemented the position of electronic or automated files as discoverable documents in their own right. This case established the basic rationale for the discovery of documentary materials which is that an order for discovery

> "should only be made where necessary, and that the court should be aware of the effectiveness of discovery as an instrument for extracting documentary evidence of the true situation and also as a means to reduce the time spent in trial eliciting what actually occurred."[73]

6.98 This built upon the dicta of McCracken J in *Hannon v Commissioners of Public Works*[74] who noted that:

> "the court is entitled to take into account the extent to which discovery of documents might become oppressive, and should be astute to ensure that the procedure of discovery is not used as a tactic in the war between the parties."[75]

(3) Creating/Regenerating Electronic Documents in Discovery

6.99 Electronic documentary materials are capable of throwing up significant questions and can potentially impose huge burdens on the producing party as was demonstrated by the 2008 English case of *Digicel v Cable and Wireless*[76] where the discovery of voluminous meta-data from electronic documents spread over a number of electronic devices added £2m to costs.

6.100 In *Dome* the Supreme Court discussed the discovery process and held that the court has the power to compel a litigant to produce electronically stored documents even where that means regenerating them which is essentially creating new representative documents. The court here built on the previous findings of the High Court in *Used Car Importers of Ireland v Minister*

---

71 [2007] IESC 59.

72 [2005] IEHC 288.

73 *Ibid,* p 19.

74 High Court, 4 April 2001.

75 *Ibid*, at p 4.

76 [2008] EWHC 2522 (Ch).

for Finance[77] which approved the need for speedy and cost effective electronic documentary discovery.

6.101 *Dome* related to the discovery of a potentially unquantifiable volume of documents. The number of documents in dispute was estimated at 20 billion call data records from electronic sources and backup tapes. These were being sought in order to show that Eircom had damaged Dome Telecom's call card business. The Supreme Court was of the opinion that such lengthy, detailed and voluminous discovery was unwarranted and disproportionate to the aims stated.

6.102 Speaking on the bulky nature of electronic documentary evidence, Geoghan J noted that as a matter of common sense the courts must adapt to their volume and "fashion appropriate orders of discovery." To achieve parity with traditional documents "it may well be necessary to direct a party to 'create documents' so as to uncover previously deleted documents" and to condense the available information so as to get a true flavour of the contents of the data base as a whole.

6.103 Commentators have noted that this case "marked a turning point in the quest to interpret discovery rules fashioned B.C. (Before Computers)."[78]

(4) Blanket Discovery of Electronic Documents

6.104 The classic statement of the test of relevance in *Peruvian Guano* was approved by the Supreme Court in *Framus v CHR Plc.*[79] The 2009 change to the Rules challenged the need for blanket discovery which had previously held sway where the documents cleared the relevance hurdle under the test found in the *Peruvian Guano* case.[80] This provides that a document ought to be discovered where it contains information which may provide help to the party seeking discovery in his litigation. The threshold to be reached was merely that the evidence sought might lead to what Brett LJ classified as "a train of inquiry which may have either of two consequences." Those were that the information would either directly or indirectly advance the party's own case or damage his opponent's.

---

77 [2006] IEHC 90.

78 Manlowe, Gregory and Borde, "Irish Supreme Court "Creates" E-Discovery: the Disappearing Line between Digital Data and Paper Documents", available at williamskastner.com/.../BordeIrishSupremeCourt.pdf.

79 [2004] 2 ILRM 439 per Murray J at 454.

80 *Compagnie Financiere du Pacifique v Peruvian Guano Co* (1882) 11 QBD 55.

6.105 The 2009 amendment of S.I. No. 93 of 2009 refocused the duty so that the party seeking discovery had to establish necessity and to stipulate the classes of documents to be discovered[81] and the purpose for each category of documents sought.[82] The discovering party is then under a duty to produce all the documents within specified classes where either an agreement has been reached or failing that where a court order has been made.[83] This reduces the burden on the producing party and prevents against "fishing" by the disputant.

6.106 The previous amendment to the Rules of the Superior Court as substituted by S.I. No. 233 of 1999 and introduced in August of that year addressed the blanket discovery of bulk documents. The 1999 Rules eliminated a vast array of duplicates and derivatives from the discovery process. These were culled under a policy of de-duplication because they are irrelevant to proceedings and represent an unnecessary outlay by the producing party. In line with the *Peruvian Guano* principles of relevance and in recognition of the ordinary rules of evidence of relevance, voluminous and bulky documents made up of duplicates and repetition are of little relevance or evidential value and can be identified and discarded as forensically identical to each other.

6.107 While electronic and automated documentary evidence may increase the difficulties associated with discovering bulky and voluminous documents, the use of electronic technologies may provide a means by which to discover documents to the court more efficiently and cheaply.

(5) Shifting the Burden of Disclosure to the Proponent

6.108 In Ireland, the 2009 amended Rules on disclosure attempt to address the burden which discovering electronic documents for production in evidence may incur. They do so in acknowledgement of the nature of electronic documents which although revolutionary as a means of storing and generating records of data quickly and cheaply, may require huge expenditure when it comes to physical production in a permanent legible form. The new Rules attempt to limit costs and introduce parity between the parties. They aim to share the burden of producing in bulk, documents which may or may not be necessary. Having to consider whether a document sought is relevant (under the pressure of having to bear the cost for its production) may prevent applications for blanket disclosure and save costs and time. The Rules reflect a more nuanced approach to the discovery of electronic documents.

---

81 Order 31, Rule 12 (1)(1).

82 Rule 12 section 1(1)(b).

83 *Taylor v Clonmel Health Care Ltd* [2004] IR 169 at 179.

6.109 Before the court orders disclosure the proponent must firstly specify and justify the classes of documents sought and the purpose for which they are sought[84] and the court will not make such an order where production would be overly burdensome and involve "significant costs" for the producing party.[85]

6.110 Where an application for extensive discovery, bordering on an application for blanket discovery is made, the court may shift the burden to produce the documents onto the proponent himself. The Rules permit a judge in these cases to facilitate the proponent's access to the opposing party's data systems so as to conduct documentary file interrogation. The party then conducts his own search using the facilities of his opponent. Though he initially bears the entirety of the expense of such a search. This provision is not an indemnity clause and these costs are recoverable against the repository of the documents at a later stage.[86] This process casts the author/maintainer of the documents as a mere facilitator and the applicant is responsible for his own search using the holding party's searching technologies and facilities.[87]

6.111 To ensure full and frank disclosure but to safeguard against one party seeking to frustrate proceedings or engage in "fishing" in a competitor's data system, the court has the power to order discovery to be undertaken by a third party who is sufficiently removed from the proceedings so as to be unbiased in the performance of his duties. This person can be appointed on consent or, failing that, appointed by the court[88] and protects sensitive and non-discoverable data.

(6) Streamlining the Production of Electronic Documents

6.112 Under the previous Rules, a court would not order revision of the documents discovered unless there were reasonable grounds for suspecting that full discovery had not been made and that documents had been omitted. This rigidity shows the trust element inherent in discovery and can be identified in cases such as *Sterling-Winthrop Group Ltd v Farben Fabriken Bayer Aktiengesellschaft.*[89]

6.113 The voluminous and bulky nature of electronically stored documents is reflected in the Rules which make provision for a more cost effective and

---

84 Order 31, Rule 12 (1)(b).

85 Order 31, Rule 12 (2)(c).

86 Order 31, r 12 (3)(d).

87 Order 31, r 12 (2)(c)(ii).

88 Order 31, r 12 (3)(b).

89 [1967] IR 97.

streamlined means of disclosure. The court has the facility to order the documents be disclosed in their raw state (electronically) which is the "searchable form in which they are held by the party ordered to make discovery".[90]

6.114 As discussed below, in the US, Canada and Australia there is a positive obligation to maintain documents once there is a reasonable anticipation of litigation. Once proceedings are contemplated, materials of potential relevance must be positively retained.

6.115 At present in Irish law there is no such complimentary provision. The Law Society considered the imposition of such a burden but determined it would be "very difficult to legislate for steps to ensure preservation of relevant documents including ESI".[91] The Committee concluded that given the motivation of most litigants towards self-preservation, there would be no value in requiring parties to issue a "hold and retain" letter[92] to accompany an application for discovery. It is likely that the 1999 and 2009 amendments to the Rules on Discovery which introduced a modified direct relevance test which requires a litigant to justify documents sought is sufficient to achieve this type of purposes of the hold and retain letter and that mandating this type of letter would be little more than a legal fiction.

(a) Presenting Electronic Evidence Electronically

6.116 Aside from making allowance for the admittance of electronic documents, the Rules of Superior Court also make provision for receiving documents electronically. An example of this can be seen in Order 63 B of the Rules of Superior Court (Competition Proceedings). S.I. No. 130 of 2005 established the Competition List in a bid to streamline proceedings. It provides that a judge hearing a case on the Competition List may of his own volition require the parties to exchange documents either amongst themselves, or crucially, to require the parties to transmit documents to the Registrar of the court electronically.[93] Order 63 B (13)(11) also permits a judge in the Commercial Court to require the case booklet to be maintained in electronic form and for this to be "lodged or served by electronic means" as the judge may specify.

---

90 Order 31, r 12 (2)(c)(i).

91 Law Society of Ireland, "*Civil Litigation, Discovery in the Electronic Age: Proposals for Change*", October 2007, p 32.

92 *Ibid*, at 32 para 6.7.

93 O 63 B, r 6 (1)(b)(x).

6.117 This style of e-disclosure also lends support to the idea of e-filing and leads the way to the introduction of fully integrated e-courts. These electronically discovered electronic documents open court proceedings to a massive amount of electronic technologies and provide for more fluid and essentially truer (by producing electronic or automated documents in their raw electronic form) forums for discovering documentary evidence. Altering the court environment in this way through true integration is preferable to choosing incremental reform of the system by the piecemeal introduction of computer technologies.

6.118 It has also been mooted that e-government will benefit from such advancements in the exchange and production of documents. It had been hoped by the Chief Executive of the Courts Service that by 2010 core technologies and facilities would have been in place to enable transactions including the payment of fines in legal proceedings and court accounting systems would be fully integrated and would take place electronically[94] and it is suggested that the time lag to fully implementing true e-courts and e-government systems is based on a combined lack of financial resources and an insufficient level of comfort with the technologies employed.

6.119 Evidence may also be offered electronically in the Commercial Court in civil litigation under this statutory instrument by video link in compliance with Order 63b of S.I. No. 130 of 2005 in connection with competition proceedings. This power to permit evidence to be recorded and transmitted by video is discretionary and evidence offered in this way may be received from within or from outside the State. There is no restriction put on the judge's discretion to make such an order and the decision does not appear to be dependent on the witness being the subject of intimidation (which are the circumstances regulating this type of evidence in analogous criminal proceedings).[95]

6.120 Under the Rules of the Superior Courts, documents may be served or exchanged electronically either among the parties or may be lodged with the court[96] and the President of the High Court may issue a practice notice prescribing the electronic media to be used. This impacts on the physical media used (discs, CD-Roms etc),[97] as well as the means by which electronic documentary meta-data can be authenticated (passwords, electronic signatures etc),[98] and the manner in which these electronic documents may be presented

---

94 Coulter, *Irish Times*, 23 March 2009.

95 O 63, r 28.

96 O 63, r 37 (a).

97 O 63, r 37(3)(b).

98 O 63, r 37 (3)(b).

to the court. All these advances mark out the Commercial Court as the most modern court and one which has been established with technology in mind and has integrated with technology to ensure "electronic service, exchange and lodgement."[99]

(7) Amendments to the Rules on Discovering Electronic Documents in England

6.121 The precise duty as to the disclosure of documents in civil litigation in England was addressed by the 1999 Woolf reforms in the Civil Procedure Rules. This replaced a system of blanket discovery with standardised disclosure mechanisms again based on the reasonableness of the search employed and judged according to the case with a primary focus on the financial burden of retrieval and the complexity of the primary litigation.

6.122 Civil Procedure Rules relating to electronic discovery and electronic documents indicate a new scheme which followed on from the suggestions arising in the Woolf reforms and represent a more liberal approach to disclosing and inspecting documents in advance of proceedings.[100]

6.123 CPR 31.6 imposes a positive duty on a party to disclose all the documents in his possession which would adversely affect his own case or another party's case or which could support another litigant's case following reasonable search.[101] The mechanism envisaged by CPR 31.6 then establishes what amounts to a file-sharing provision.

6.124 Where an opposing litigant receives documents under these provisions he is effectively barred from disputing the authenticity of the documents unless he does so immediately upon receipt of them. Any challenge available to him is by means of service of a notice requiring that the other party take steps to prove the document at trial.[102]

---

99 O, 63 A, r 31.

100 CPR 31.16.

101 CPR 31.8.

102 CPR 32.19.

(8) Compelling Disclosure of Encrypted Computer Files

6.125 The 2008 proceedings in *R v S and Another*[103] concerned the investigation of files which had been encrypted by the respondents. Charges were brought under the *Terrorism Act 2000*. An order for disclosure was made under section 49(a) of the *Regulation of Investigatory Powers Act 2000* which had created the power to compel disclosure of locked data as being "any electronic data which, without the key to the data (a) cannot, or cannot readily, be accessed, or (b) cannot, or cannot readily be put into an intelligible form". A facility is made available under section 49 (b) by which a person with sufficient authority and permission who believes

> "(a) that a key to the protected information is in the possession of any person",

6.126 Can obtain an order for disclosure where this is necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty.[104] That person may move to access this information and have it produced to him in a legible form.[105]

6.127 S and A were served with section 49 notices in order that they be compelled to disclose the key code for the encrypted file which was necessary to render the file intelligible. The necessity in relation to this was expressed by reference to national security. Both S and A disregarded the order and claimed privilege against self-incrimination.

6.128 Charges were brought following their refusal to disclose. This prompted a judicial discussion on the privilege, interference with which was held to be "proportionate and permissible" because the information was already in the hands of the authorities but was in an incomprehensible form. The key was necessary to "enable the otherwise unreadable to be read (which) was a legitimate objective which dealt with a recognised problem of encryption".[106] The order to compel was thus legitimate given the stated aim of the *Regulation of Investigatory Powers Act 2000* and as a means to regulate the practice of encryption.

---

103 [2008] EWCA Crim 2177.

104 Section 49(b)(ii) of the *Regulation of Investigatory Powers Act 2000.*

105 As specified under Schedule 2 of the Act.

106 [2008] EWCA Crim 2177, para 25.

6.129 The key was in and of itself a fact.[107] Under these circumstances it would not engage the privilege against self-incrimination as the key was evidence independent of the wishes of the respondent.[108]

6.130 In *R v S and Another,* the key was of great importance to enable the information to be available in a legible and "intelligible form that it was in prior to encryption; the material in the possession of the police will simply be revealed for what it is."[109] It was not in itself an admission of guilt. The key as a fact was to be disclosed in the interests of national security and the prevention of crime and the court held that this in no way prejudiced the trial unfairly as without the key the information would remain inert.

(9) Discovering Electronic Documents in Canada

6.131 Discovery in other jurisdictions is informed by international principles and places great emphasis not only on the good faith of the parties but also on the reasonableness of the search undertaken. This reasonableness is in turn inextricably linked with the good faith principle upon which documents are retained or discovered.

6.132 The 2007 Sedona Canada Conference specifically addressed international standards of electronic documentary discovery. These principles

---

107 A parallel was drawn between the key to decrypt the record and a blood or urine sample which can be compelled under the *Road Traffic Act 2000*. It is merely a tool by which to gain access to the information required. This was without prejudice to the position of the key as a tool which tended to establish that the respondent was knowingly in possession of illegal material which had been deliberately encrypted so as to scupper any attempts to uncover it. See further *Re Boucher* (2007) WL 4246473 (District Court of Vermont). Here the act of producing fingerprints or blood samples was deemed not to attract the privilege for similar reasons being that the samples would facilitate the investigation of the crime.

108 *Attorney General's Reference (No. 7 of 2000)* [2001] EWCA Crim 888; *R v Kearns* [2002] EWCA Crim 748; and *R v Dhaliwal* (2004) 2 Cr App R 307 which expressly approved *R v Kearns* in identifying the distinction between "the compulsory production of documents or other material which have an existence independent of the will of the suspect or accused person and statements that he has had to make under compulsion. In the former case there is no infringement of the right to silence and the right not to incriminate oneself. In the latter case there could be."

109 [2008] EWCA Crim 2177, para 25.

emphasise a proactive approach to the retention of documents which "it is reasonable to expect...may be relevant to future litigation."[110]

6.133 The nature of documentary discovery, the trust which it places on litigants and the position it occupies in relation to all litigation was emphasised in Canada in the 2002 case of *Doust v Schatz*[111] where the court stated:

> "the integrity of the administration of justice in both civil and criminal matters depends on a large part on the honesty of parties and witnesses. Spoliation of relevant documents and production of documents in civil actions contemplates that relevant documents will be preserved and produced in accordance with the requirements of the law."

(10) Imposing Sanctions for Refusal to Disclose in the US

6.134 While issues surrounding the discovery of electronically generated documentary evidence have been gaining significance for some time, the legal framework regulating this field has been slow to emerge. In the US however, matters concerning the discovery and use of technological evidence at trial originated in the 60s and 70s when businesses and commerce first began to use computers on a large scale operational level. This led to the US Advisory Committee recommending in 1970 that existing documentary rules did not adequately address matters peculiar to electronic documentary evidence and which impacted on its admissibility including circumstances relating to the discovery of such documentary materials. Rule 34 of the Federal Rules of Civil Procedure now govern the production of documents and extend to this include electronically stored information (ESI).

6.135 In acknowledgement of the central role of electronic documentary evidence to proceedings in the US, uncooperative litigants who fail to produce electronic evidence are liable to court sanctions. This has been the situation since electronic evidence was in its infancy. In 1993 in *Crown Life Insurance Co. v Craig*[112] the US Seventh Circuit upheld the sanctions which were imposed where a party refused to furnish the court with the requested computer records and had provided only hard copy documents which did not contain copies of electronic evidence earlier referred to.[113] Crown's claim that this data was inaccessible and remained in raw digital form was not accepted. On appeal the

---

110 Sedona Canada Conference 2007, Comment 4 c, p 17.

111 (2002) 227 Sask R 1 (CA).

112 995 F 2.d 1376, 1377, 1380-84 (7th Cir. 1993).

113 *Ibid*, at 1376, 1377, 1380-84.

court held that Crown had a duty to disclose the records, regardless of their form.

(11) Developments on the Rules on Discovering Electronic Documents in Australia

6.136 There are more contemporary cases concerning the voluminous nature of electronic documents affecting their disclosure. The notably significant case of *British American Tobacco Australian Services v McCabe*[114] recognised the potential for electronic or automated documents to be altered or destroyed in defiance of obligations to disclose. The Supreme Court of Victoria examined the circumstances arising out of the failure of British American Tobacco to log documents sought in discovery. These "Cremona documents" so called because they were connected to an earlier civil suit of the that name had been subject to a policy of systematic destruction extending to a massive quantity of damaging documentary evidence in order to prevent its admittance as evidence.

6.137 The Court held that BAT had destroyed potentially significant documents which were easily foreseeable as being necessary evidence in a civil suit and which would have benefitted the respendent in her case. This was found to have been a deliberate policy directed at preventing the litigant from pursuing a case and which impacted on her right to a fair trial. As far back as 1985 solicitors acting for BAT's then parent company had anticipated a "wave of litigation" and a policy of destroying sensitive electronic documents had been undertaken under the guise of "an apparently innocent house-keeping arrangement".

6.138 This judgment was however overturned on appeal in *British American Tobacco Australia Services Ltd v Cowell*[115] and no other action had been taken when the respondent died. The case remains however, as a marker of the shift towards pro-active document retention where the Victorian Court of Appeal recognised the seriousness of the destruction policy in which "not only were the documents discovered in the Cremona litigation destroyed, at least in the main, so too was the database, denying the defendant the ability to describe the documents in question."

6.139 In *R v Ensbey; ex parte AG (Qld),*[116] the Supreme Court of Queensland held that where a person can reasonably foresee that a document

---

114 [2002] VSC 73.

115 [2002] VSCA 197.

116 [2004] QCA 335.

may be needed as evidence in any possible future litigation, they cannot legally destroy the record.

6.140 Legislation followed in the wake of the *McCabe* case in the form of the *Crimes (Document Destruction) Act 2006 (Victoria)* which amended provisions in the *Crimes Act 1958* relating to the destruction of evidence which "is reasonably likely to be, required in evidence in a legal proceeding."[117] These legislative provisions addressed the need to retain and maintain documents for evidence. While the knowing destruction of evidence was already actionable and amounted to the criminal offence of attempting to pervert the course of justice, the new provisions made the operation of the law to business enterprises clear. A further statutory provision in the *Evidence (Document Unavailability) Act 2006* amended the *Evidence Act 1995* and granted courts wide powers when it comes to discovering documents in civil proceedings. Powers under the new provisions include the power to draw adverse inferences against a party for the unavailability of documents and reversing the evidential burden of proof on the determination of documents.

6.141 In 2000 the Federal Court in Australia issued a practice note on the means by which electronic technologies could be put to use to streamline the disclosure process as well as during the course of litigation. This laid down variables for the discovery of voluminous documents and established a threshold which would engage the use of technologies. Where the discovery was to relate to 500 or more documents, the parties were to be encouraged to "exchange documents and indexes in electronic format".[118]

6.142 The practice note also made provision for the electronic exchange of court documents which can be filed with the court prior to the hearing. While this will undoubtedly speed up the process, it is not intended as a means by which to replace hard copy files and is instead phrased in a way so that electronic filing supplements the hard copy documentation.

6.143 This 2000 practice note was superseded by a 2009 practice note issued form the Chief Justice of Australia. The 2009 document advances the position of e-discovery even further and directs litigants to suitable protocols and checklists to be followed during the discovery process. This 2009 note mandates disclosure by electronic means where the volume of documents has reached just 200 pieces which have been generated or are stored electronically or are automatically generated and held within data systems.

---

117 Section 254.

118 Guidelines for the Use of Information Technology in Litigation in Any Civil Matter, Part 1 (4).

6.144 During the Second Reading prior to the introduction of the Australian *Evidence (Document Unavailability) Act*, it was noted that the motivation for these new measures was the necessity of having relevant documentary evidence adduced before the court as "material relevant to civil justice proceedings (must) be available to the court for the proper and fair resolution of those proceedings."[119]

D Regulating Documentary Evidence in the Context of Commercial Transactions

(1) Introduction

6.145 The growth in the use of electronic communications as a medium for both business and non-commercial transactions has opened up new avenues which can be exploited and used to perpetrate crime and has resulted in a strain of Cybercrime hitherto unknown and unpoliced. This includes incidences of fraud, theft of intellectual property or confidential data infiltration and harassment with the aid of a computer. Due to the relatively low rate of internet use in Ireland there is a dearth of technical and legal knowledge on how to protect society from the influence of Cybercrime and on a more simplistic level how to authenticate computer derived evidence for the purposes of litigation.

(2) Authentication of Electronic Documentation in the Context of Commerce and Industry for Admission into Evidence in Ireland

6.146 Many businesses and consumers are wary of conducting business over the Internet due to a perceived lack of security. Transactions conducted over the internet and in e-format are a prime target for attempts at unauthorised access, alteration and destruction of both data and systems.[120]

6.147 Digital evidence may give rise to significant issues arising from reliability and authentication given the opportunities (whether or not they can actually be capitalised on) to infiltrate and augment files by persons with access to the disputed system or even by third parties through the transmission of viruses. The extent to which a document is vulnerable to risk in this regard is contingent upon a multiplicity of factors including the size of the class of individuals with access to the computer/machine as well as the level and sufficiency of security and encryptions used to secure the digital devices or resulting documents.

---

119 The Hon Rob Hulls, Second Reading Speech, Legislative Assembly of Victoria, 31 May 2006 available at http://tex.parliament.vic.gov.au/bin/texhtmlt.

120 OECD (1999) Joint OECD-Private Sector Workshop on Electronic Authentication. Available athttp://www.oecd.org//dsti/sti/it/secur/act/wksp-auth.htm.

6.148 The *Electronic Commerce Act 2000* is another aspect of the multi-pronged legislative approach to the regulation of commercial transactions and contractual formation with a knock on effect on the law of evidence. It consolidates elements of the pre-existing common law of contract and further implements much of the EU Directive on e-signatures- Dir 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on legal matters of information society services with a particular emphasis on electronic commerce.[121] The scope of the directive is to ensure a "high level of community legal integrity in order to establish a real area without internal borders for information society services."[122]

6.149 The *Electronic Commerce Act 2000* is a means by which to establish a high watermark for consumer confidence by laying down a general framework through which to conduct electronic transactions in the internal market. To facilitate both domestic and international commercial electronic transactions the Act regulates and thereby strengthens the authority of various electronic and digital media. It does so by establishing a legal framework under which to recognise and legitimate the authenticity and reliability of digital data exchanges and provides for the accreditation of documentary-associated certifications.

6.150 To this end it provides for the legal recognition of electronic contracts, electronic writing, electronic signatures and other original information generated in e-form.[123]

6.151 The Act lays out provisions for a thorough and comprehensive system with which to regulate electronic contracts. It lays out a parallel electronic commercial regime. Section 19 places digital contracts on a par with their paper-based equivalent, section 20 specifies the framework to adapt traditional contractual concepts to function in an electronic environment. It provides a means for establishing the receipt and acceptance of transactions removing the motivation for much legal wrangling which would have emerged in its absence. Likewise section 21 clarifies the legal position on determining the time and place of dispatch and receipt of electronic communications.

---

121 Specific aspects of the *2000 EU Directive on Electronic Commerce, Directive 2000/31/EC*, have also been implemented by the *European Communities (Directive 2000/31/EC) Regulations 2003 (SI No.68 of 2003)*, as amended by the *European Communities (Amendment of S.I. No. 68 of 2003) Regulations 2004 (SI No.490 of 2004)*. The 2003 Regulations, as amended, complement and, in part, adapt the general provisions in the *Electronic Commerce Act 2000*.

122 Directive 2000/31/EC, Article 3.

123 Long Title to the 2000 Act.

6.152 To integrate electronic documents into the cohesive law of evidence, the Act attempts to remove any latent prejudices against electronically generated documentary evidence with section 9 specifying that no information, including that incorporated by reference "is to be denied legal effect, validity or enforceability solely on the grounds that it is wholly or partly in electronic form, whether as an electronic communication or otherwise".[124]

6.153 The Act attempts to cover every situation and contingency providing that whatever the channel of distribution, whether the document is communicated by an individual or public body required by the law to so transmit, should an existing law require a document to be in writing, that requirement is deemed satisfied by an electronic document.[125] Under section 17, an electronic document is sufficient and acceptable to satisfy any legal obligation on an individual or public body to supply data "if there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form"[126] so long as it is, (perhaps rather subjectively) "intelligible" to the intended recipient[127] and once again where the consent of the intended recipient is sought prior to the transactions.[128]

6.154 Thus while the legislation seems to envisage total acceptance of electronic media, its provisions could be seen as retaining a preference for traditional paper-based documents. This can be seen in the proviso that prior to transmittal, steps must be taken to ascertain whether the intended recipient has consented to the information being given in that form.[129] This would seem to nullify the possibility of streamlining the process of communicating information and exchanging documents which would otherwise be of benefit when transferring documents electronically. Rather than yield to the balance of convenience, the legislation instead seems malleable to the personal preferences of the end-user and further imposes other restrictions on the evidence which is acceptable only where the electronic document in question has remained complete and is unaltered.

---

124 Section 9.

125 Section 17.

126 Section 17 (2) (a).

127 Section 17 (2) (b).

128 Section 17 (2) (e).

129 Section C.

(3) Admissibility of Electronic Evidence under the Electronic Commerce Act 2000

6.155 Section 22 of the *Electronic Commerce Act 2000* addresses the admissibility of evidence in electronic form. It does so by essentially seeking to guarantee that electronic evidence achieves sufficient evidential certainty to pass over the threshold of admissibility which must be established by all documentary evidence. It aims to ensure this legal validity by creating a climate where the evidential value of an electronic or automated document is above any reproach based exclusively on its electronic format. Section 22 states:

> "In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility in evidence of—
>
> (a) an electronic communication, an electronic form of a document, an electronic contract, or writing in electronic form—
>
> (i) on the sole ground that it is an electronic communication, an electronic form of a document, an electronic contract, or writing in electronic form, or
>
> (ii) if it is the best evidence that the person or public body adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form, or
>
> (b) an electronic signature—
>
> (i) on the sole ground that the signature is in electronic form, or is not an advanced electronic signature, or is not based on a qualified certificate, or is not based on a qualified certificate issued by an accredited certification service provider, or is not created by a secure signature creation device, or
>
> (ii) if it is the best evidence that the person or public body adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form."

6.156 While section 22 of the 2000 Act protects digitally derived evidence from attack solely on the basis that it takes that form it stops short of establishing such evidence as conclusive best evidence. Instead digital evidence must first establish itself as admissible under existing rules of evidence.

6.157 In assessing the evidential weight of an electronic data message or electronic document, the reliability of the manner in which it was generated, stored or communicated, the reliability of the manner in which its originator was identified will all be considered in attaching evidential weight. The 2000 Act does not, however, specifically provide for evidence to be received in its raw

digital state. This again reflects the preference for hard-copy paper documents and reflects the court infrastructure which in the main is not sufficiently integrated to enable documents to be admitted electronically in all litigation although this is now being addressed in initiatives such as the Commercial Courts e-infrastructure which has the facility to receive documents which have been logged electronically as evidence.

6.158 The extent to which the legislature intended to pre-legitimate electronic textual documents can be seen from the broad and inclusive definitions offered in the legislation. From this perspective, section 22 is of importance and its potential ambit very wide. On the most basic level of digital currency, "electronic" is described as including:

> "electrical, digital, magnetic, optical, electro-magnetic, biometric, photonic and any other form of related technology" and information is likewise broadly drawn and embraces data, all forms of writing and other text, images (including maps and cartographic material), sound, codes, computer programmes, software, databases and speech".[130]

6.159 These aspects of the *Electronic Commerce Act* are however open to criticism. Despite its widely inclusive definitions, the Act does not incorporate any safeguards on the admissibility of electronic evidence. The statute does not expressly modify any statutory rule relating to admissibility of electronic data massages or electronic documents.

6.160 To remedy any of these issues expert evidence may be called upon. However a point of contention inherent in section 22 is the failure of the provision to require advance notice of the use of digital evidence. This could significantly impede an opposing party's ability to challenge any issues arising from evidence tendered under the section where they are unaware of their opponent's intention to offer such evidence.

(a) How is Digital Evidence Authenticated under the Act?

6.161 The 2000 Act as a whole is an aid in helping to establishing (for authentication purposes), the integrity of an electronically derived document. For example section 17, which concerns the presentation of electronic originals, provides that information may be introduced or retained where "there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form".

6.162 The means of assessing the integrity of the impugned document includes criteria focusing on whether the information has remained complete and unaltered. The section acknowledges the every-day fallibilities of electronic

---

130 *Electronic Commerce Act 2000,* section 2.

devices and allows for any discrepancies which may arise from any such technical glitches. However it provides that the integrity of the documentary evidence in question is not prejudiced by these irregularities which may have arisen in the normal course of generating, communicating or processing the data. The standard of reliability is extremely subjective and dictated to by the circumstances in which the information was generated.[131]

(b) Documentary Evidence of Internet Communications under the Electronic Commerce Act 2000

6.163 Where transactions are conducted through an e-format, authorities must be able to trace the website to a primary originating user and link those activities with the real world physical parties behind it. Problems arise where the inherent reliability of certain communication mediums are in question. Websites represent a good example of this. The true identity of the party behind the website can be easily concealed. Authentication of electronic or automated documents focuses on establishing the validity of the alleged identity of the person behind the computer or indeed the validity of the device used to generate the document. It relates therefore to both human and electronic identification and how to establish confidence in these so as to have the information admitted as evidence in proceedings.

(i) Domain Names

6.164 Section 31 of the *Electronic Commerce Act 2000* deals with the registration of domain names. It empowers the Minister for Finance to establish regimes for authorisation, prohibition or regulation through registration and use of the "i.e. domain name" in the State.[132] This can be seen as an effort to streamline and enhance the functionality as well as reliability and security of e-transactions originating in Ireland and to increase confidence in the Irish system on a national and global scale.

6.165 This goes some way to remedying issues which arise as to the authenticity or otherwise of internet-based activities. It also introduces the body known as the Internet Corporation for Assigned Names and Numbers (ICANN) into Irish evidential parlance. This may become more relevant as electronic documentation issues arise more in litigation. The ICANN is a body which attempts to coordinate on a pan-global level, the internet's systems of identification. Its ultimate goal is "to ensure the stable and secure operation of

---

131 Section 17 (4)(b).

132 This "i.e. domain name" refers to the global domain name system assigned to Ireland according to the two-letter code in the International Standard ISO 3166-1 (Codes for Representation of Names of Countries and their Subdivision) of the International Organisation for Standardisation.

the Internet's unique identifier systems."[133] The ICANN operates by coordinating the allocation of the three sets of unique identifiers for the internet namely:

1. Domain names (forming a system referred to as "DNS");

2. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and

3. Protocol port and parameter numbers.

6.166 It also acts as a watch-dog of the operation of the DNS root name server system. Section 31 of the 2000 Act authories the making of Regulations which may designate registration authorities,[134] prescribe a satisfactory form of registration,[135] define the period for which registration can legitimately continue in force,[136] dictate the terms, periods and circumstances for renewal or refusal to issue or refuse registration.[137] It provides for mechanisms of appeal[138] and determines appropriate levels of fees payable upon the grant or renewal of registration and the time and manner in which such fees are to be paid.[139] Section 31 thereby cedes to the Minister all matters relating to the regulation and registration of domain names. It invests him with significant powers and control in an effort to stabilise public confidence in web-commerce yet it cedes the actual business of establishing the integrity and authenticity of certification to designated accreditation service providers.[140]

(ii) Certification Authorities

6.167 A digital certificate is essentially an electronic credential card issued to both individuals and corporate entities. It enables them to prove their credentials and permits them to conduct business or other transactions through an e-format. A Certification Authority (CA) issues the certificate detailing the

---

133 The ICANN homepage can be accessed at http://www.icann.org.

134 Section 31 (2) (a).

135 Section 31 (2) (b).

136 Section 31 (2) (c).

137 Section 31 (2) (d) and (e).

138 Section 31 (2) (f).

139 Section 31 (2) (g).

140 These is their turn are responsible under the Act for ensuring the accuracy of all information to be contained in the certificate, that the signatory party identified in the certificate held the signature creation device corresponding to the signature verification device given or identified in the certificate (section 30 (2) (b)).

user's name, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate issuing authority so that a recipient can verify that the certificate is real.[141] Under the *Electronic Commerce Act 2000* Ireland seems to operate a registration authority system which authenticates the identities of individuals and authorities who apply for digital certificates. This is considered in more detail in Chapter 4.

(iii) Recognition of Electronic Signatures

6.168 The *Electronic Commerce Act 2000* makes similar allowances for the recognition of e-signatures where required by "law or otherwise"[142] but appears again to be premised on the receiver's consent to the use of an electronic signature. The recipient has the option of requiring that the document and accompanying authenticating e-signature be in accordance with specified idiosyncratic information technology and procedural requirements "including that it be an advanced electronic signature, that it be based on a qualified certificate, that it be issued by an accredited certification service provider or that it be created by a secure signature creation device".[143]

6.169 The 2000 Act thus raises the status of an electronic signature to the equivalent of a manually executed signature provided by an individual who signs a primary, written document. To do this it provides a mechanism through which the electronic signature can be proven by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, was adhered to. There is also an element of public scrutiny involved under section 14 of the 2000 Act for signatures, which require witnessing to the extent that the public body's requirements for issuing e-signatures have been met, have been made public and are "objective, transparent, proportionate and non-discriminatory" in their application.[144]

6.170 Thus under the 2000 Act, for evidentiary purposes, an electronic document shall be the functional equivalent of a written document. The basis for authenticating these types of documents is to have regard to all relevant circumstances.[145] Where the law requires that a document be presented or retained in its original form, that requirement is satisfied by an electronic document where there exists a reliable undertaking as to its integrity dating from

---

141 DeVeau P, *VPN = Very Private News.* (1999) America's Network, Volume 103(21) May 21, p16.

142 Section 13 (1).

143 Section 13 (2) (a).

144 Section 14 (2) (a).

145 Section 17 (4) (b).

the time when it was first produced in its end form. Under the 2000 Act, the criteria for assessing the integrity of a document presented in a digital form are dependent on whether the information has remained "complete and unaltered" subject to any "addition of any endorsement or change which arises in the normal course of generating, communicating, processing, sending, receiving, recording, storing or displaying" any such document.[146]

6.171 The Act shifts the responsibility for authentication for the purposes of admissibility of electronic or automated documentary evidence onto accreditation organisations specialising in certification. Yet regulation under the Act as it relates to this is patchy with no legislatively imposed standardisation. Indeed the need if any to require certification in any particular transaction is not mandatory. This is outlined in section 29 (1) where a "person or public body is not required to obtain the prior authority of any other person or public body to provide certification or other services relating to electronic signatures." The Minister is instead empowered to establish accreditation schemes but there is no legislative impetus to comply.

6.172 The system is instead predicated on ad hoc compliance with voluntary accreditation and certification service providers which could leave the system open to abuse. The Act goes some way to avoid this situation through section 6 on the prosecution of offences and builds on this in section 7 where the issue of blue-collar crime is broached. This section addresses offences perpetrated by corporate bodies and goes further, lifting the commercial shield and exposing directorial and managerial wrong-doing by which "that person,[147] as well as the body corporate, shall be guilty of an offence."

(iv) Summary and Potential for Reform

6.173 Section 25 is engineered towards the prohibition of fraud and misuse of electronic signatures and signature creation devices. It details offences for the unauthorised access, recreation or acquisition of e-signatures or creation devices,[148] as well as offences of knowingly altering, disclosing or using a signature creation device without consent[149] or misrepresentation of a person's or public body's identity or authorisation in requesting or accepting a certificate

---

146 Section 17 (4) (a).

147 "Person" being a director, shadow director (as defined in section 3(1) of the *Companies Act 1990*), manager, secretary or other officer of the body corporate, or a person who was purporting to act in any such capacity" as per section 7 *Electronic Commerce Act 2000*.

148 Section 25 (a).

149 Section 25 (b).

or in requesting suspension or revocation of a certificate.[150] Although this would appear to be a comprehensive list it is debatable whether the Act goes far enough to safeguard electronic documents. The Act does not lay out a regulatory regime for authenticating and admitting documents. It leaves this to accreditation and certification holders and compliance with these remains on a voluntary basis.[151]

6.174 Any further legislative instruments for deciding on the admissibility of documentary evidence would take the form of a dictate that authentication procedures should include satisfying the court of the validity of the claimant's identity or evidence substantiating the reliability of the mechanical device in question for processing information or creating signatures. These could be satisfied in the case of electronic or automated documents by determining whether the device generating them was functioning correctly and by presenting proof that an appropriate security measures and procedures have been adhered to in order to establish and verify the integrity of the document.

6.175 This would go further to safeguard documents and would place a proactive duty on those producing or retaining such documents. It would instil user confidence and go a long way towards the detection and elimination of fraud where any documents which had been tampered with would be stopped at the point of entry before they have time to infiltrate systems. This could be achieved with the use of algorithms or codes, identifying words or numbers, encryptions, or acknowledgement procedures.

6.176 With regard to securing the admissibility of documents dependent on electronic signatures, these signatures could be authenticated by furnishing proof in the form of an identifying letter, character or other symbol in electronic form representing the person's name and specifically allotted to them. This measure could also be satisfied by the imposition and uptake of appropriate security procedures and notarisation systems to be employed by the party depending on the "signed" document with an express intention to authenticate the document as produced in its electronic form.

(4) Conclusion

6.177 Legislation which addresses electronic and automated evidence is addressed to technologies which are in continuing flux, the evolution of which is unforeseeable. While this unknown element of technology poses some questions it does not mean to imply that such technologies are immune to being legislated for. Paper documents are more readily available and therefore just as amenable to falsification and alteration. It is merely the authenticating tools for

---

150 Section 25 (d).

151 As discussed in Chapter 7.

paper documents with which we are more familiar and ready to base our assessment on. New PKI software is being developed with which to detect computerised manipulations. At present however, it may be that the instruments to validate electronic or automated documents are unknown and therefore treated with a level of mistrust. This perception may shift as they become better understood and are more widely used.

6.178 Examples include "message digests" which involves attaching a unique tracer to an electronic document. Any subsequent alteration can be identified by comparing an original digest with a new tracer which is based on the file at hand. By means of comparison it can be determined whether the information has been changed in any way as a different output value will be produced.[152] Such a system of checks ensures documentary integrity can be verified by the use of this message digest, which generates a short fixed length value known as a hash. A hash function is a transformation that reduces a large data message to one of a more comprehensible size thus reducing it to a fixed length.[153] There is no way to decrypt a hash, nor any known way to create two different messages that generate the same hash.[154]

6.179 It must also be kept in mind that courts are adopting a more inclusionary approach, which is suggested by the growth of categories of exceptions accommodating evidence otherwise inadmissible under the Hearsay Rule. This would seem to suggest that courts are, by and large, concerned less with issues of authentication which affect admissibility rather than with the probity of the proposed document and the disputed evidence which must be of relevance to the fact in issue. Where potential evidence is identified as superfluous or irrelevant it will not be entertained. In determining the admissibility and evidential weight of a piece of documentary or electronic or automated evidence, regard should be had to the reliability of the manner in which the document was created, transmitted or maintained, the process by which the reliability of the integrity of the document can be assessed, and observing the requirement that the best available evidence is adduced.

6.180 There are few judicial discussions of the admissibility of electronic evidence to suggest many difficulties being thrown up by these documentary instruments. There are therefore either relatively few in number or these issues are being disposed of on consent by the parties prior to the commencement of proceedings before the court.

---

152 See below paragraph 7.64.

153 ITB Journal, Issue Number 3, May 2001 p 31. Also see further- Chapter 7.

154 Deitel, Deitel, and Nieto (2001) *e-Business & e-Commerce: How to Program*. Prentice Hall NJ.

6.181 The Commission does not wish to introduce prescriptive criteria but does wish to encourage a consistent approach to security procedures and practices surrounding the creation, maintenance and authentication of electronic signatures. Any would be infringements would then fall to be handled uniformly and through designated procedures. This could include a presumption that in the absence of evidence to the contrary, the integrity of the system in which the document is stored, generated or through which it is communicated is admissible. This would be followed by expert evidence that at all material times the system or mechanical devise was functioning correctly, and that its operation did not in any fashion affect the composition and integrity of the impugned document. This would speak to the integrity of the documentary evidence. In the absence of other grounds (with the onus on the proffering party) to cast doubt on the operation of the system, a path towards the authentication of the document would be established. In this situation, it would become the norm that the party offering the evidence would be relieved of any duty to lead evidence in order to demonstrate that the system was working properly thus alleviating them of any onerous burden of front loading proof as well as any accompanying costs.

6.182 The Commission is of the opinion that any legislative framework would include a provision providing that the presumption of regularity would apply to admit the reliability of the electronic device for admissibility. By refusing to impose a higher standard for laying the foundation prior to admitting electronic documentary evidence the evidence would be admitted unless there was rebuttal evidence to establish that the electronic device was not operating correctly. The Commission thus recommends that because of the difficulties inherent in creating legislation based on technological criteria, no special evidential regime needs to be introduced to govern the admissibility of computer-generated documents.

6.183 The Commission provisionally recommends that in light of the Commission's view that the law should be technologically-neutral, no special evidential regime should be introduced to govern the admissibility of computer-generated documents.

6.184 The Commission invites submissions as to whether in connection with electronic and automated documentary evidence a distinction should be made as between an "original" and a derivative in admitting documentary evidence.

CHAPTER 7 CERTIFYING AND VERIFYING ELECTRONIC DOCUMENTS

7.01 In this Chapter, the Commission examines the processes for authenticating, certifying and verifying traditional, paper-based documents and also for electronic documents. The admissibility of electronic documentary records is of relevance to all areas of the law. Issues as to the admissibility of electronic documents are particularly amenable to understanding when examined in the context of electronic commerce as they are also integral to the facilitation of this method of transacting. Verification of a paper document has traditionally been done through a signature or a seal. Similarly, electronic signatures have been used to verify and authenticate electronic documents. The 1999 EU Electronic Signatures Directive,[1] which followed the broad approach adopted in comparable laws in, for example, the United States, was implemented in Irish law in the *Electronic Commerce Act 2000*. In Part A, the Commission examines existing law concerning what constitutes a "signature" and "signing" for the purposes of traditional documents.

7.02 In Part B, the Commission examines the emergence of digital signatures and the increasing use of digital signatures to verify and authenticate electronic documents. It also considers how these signatures differ from manual signing and the need and means by which to regulate them. It also discusses the volatility of electronic documents and how electronic signing can be used to verify and authenticate the document and identify the parties behind what appear to be mutable documents for evidential purposes.

7.03 In Part C, the Commission examines the different technologies and legislative and regulatory frameworks which have been enacted in this area to verify and authenticate electronic documents. It explains the different strains of electronic signature and the mechanics of the technologies (PKI, hash functions, message digests and key pairs) employed both domestically and internationally. Part C looks at the three broad approaches which these regulatory frameworks follow - the minimalist approach, the hybrid approach and the mandatory/prescriptive approach, and how these operate in various jurisdictions.

---

1 Directive 1999/93/EC.

7.04 In Part D, the Commission discusses the current use and regulation of electronic signatures in Ireland and examines in detail the provisions of the *Electronic Commerce Act 2000* which implemented the 1999 EU Electronic Signatures Directive. This also looks at the use, formalities and prevalence of e-signatures in various jurisdictions and the use of certification to identify the parties and verify the documentary instruments concerned.

A The Legal Significance of Signatures and Signing

(1) Signatures and traditional documents

7.05 It is long-established that verification and authentication of a paper document can be done through a signature. In earlier times when adult literacy was the exception rather than the norm, a mark in the form of a cross was often used for this purpose. In the modern era, personal signatures remain an important method of verifying and authenticating business and public documents. In the corporate context signatures are often also used in conjunction with corporate seals.

(2) Specific legislation that requires writing and a "signature"

7.06 Even though there is no general requirement in Irish law that contracts be in writing or that documents must be signed, in practice, many contracts are made in writing and many documents are signed. There are a number of specific statutory requirements that certain contracts be evidenced in writing, and which also require a signature.

7.07 For example, section 51 of the *Land and Conveyancing Law Reform Act 2009* states that proceedings to enforce a contract for the sale of land can only be brought where the contract "or some memorandum or note of it, is in writing and signed by the person against whom the action is brought or that person's authorised agent." Section 51 of the 2009 Act replaced the similar long-standing requirement in section 2 of the *Statute of Frauds (Ireland) 1695.*

7.08 Section 2 of the 1695 Act, written in somewhat archaic language, continues to require similar requirements as to a written note and signing in respect of contracts of indemnity[2] and other legislation requires, for example, that a will be "signed."

7.09 In a similar vein, the *Terms of Employment (Information) Act 1994*, as amended, requires that the essential terms of most contracts of employment be put in writing by the employer. Section 3(4) of the 1994 Act states that the written statement of terms "shall be signed and dated by or on behalf of the employer."

[2] See generally, Clark, *Contract Law in Ireland* 6th ed (Thomson Round Hall, 2008).

7.10 The Commission notes that the *Interpretation Act 2005* provides that in any legislation, the word "writing":

> "includes printing, typewriting, lithography, photography, and other modes of representing or reproducing words in visible form and any information kept in a non-legible form, whether stored electronically or otherwise, which is capable by any means of being reproduced in a legible form."

7.11 In that respect, of course, the 2005 Act provides for the recognition of digital writing.

7.12 The Commission also notes that none of these statutory provisions, including the *Interpretation Act 2005*, defines what a "signature" is, or what constitutes "signing," but the essential factors involved in this have been established through case law, to which the Commission now turns.

(3) The meaning of a "signature" for traditional documents

7.13 Long-standing case law has established that a signature usually involves a person writing their own name, or mark, on a document with the intention of authenticating it, whether to indicate it is theirs - such as a will - or that it is legally binding on them – such as a contract.

7.14 Thus, in the High Court decision *Dundalk AFC Interim Co Ltd v FAI National League*,[3] Finnegan J quoted with approval the following passage from *Stroud's Judicial Dictionary*:[4]

> "Speaking generally, a signature is the writing, or otherwise affixing, a person's name, or a mark to represent his name, by himself, or by his authority...[5] with the intention of authenticating a document as being that of, or as binding on, the person whose name or mark is so written or affixed."

7.15 In the *Dundalk AFC* case, Finnegan J had to consider whether a football player had been properly registered with the plaintiff club under the defendant league's rules. Those rules stated that a person is properly registered when "he has signed a registration form." In this case, the player had not

---

3 [2001] 1 IR 434.

4 *Stroud's Judicial Dictionary of Words and Phrases* 6th ed (Sweet & Maxwell, 2000), Vol 3, p 2449.

5 Finnegan J omitted the reference here in *Stroud's Judicial Dictionary* to *R v Justices of Kent* (1874) LR 8 QB 305 in support of this summary of the law. As noted in the text, Finnegan J went on to refer with approval to a passage from the judgment of Blackburn J in the *Justices of Kent* case.

personally signed the registration form but he had authorised the club's manager to do so, and the manager had signed it on this basis. As already indicated, Finnegan J quoted with approval the definition in *Stroud's Judicial Dictionary* and he also cited a passage from the English High Court in *R v Kent Justices*[6] in which Blackburn J stated:

> "No doubt at common law, where a person authorises another to sign for him, the signature of the person so signing is the signature of the person authorising it."

7.16 On this basis, Finnegan J concluded that the registration form had been "signed" by the player and that he had been properly registered.

7.17 As indicated, in analysing the meaning of "signature", Finnegan J referred with approval to the common law developed in English courts. The Commission now turns to discuss some other decisions of the English courts where the general common law approach has been applied in specific statutory settings.

7.18 In *Goodman v J Eban*[7] the English Court of Appeal addressed both the form of signature and the means by which it was affixed. The case concerned whether the plaintiff, a solicitor, had "signed" a bill of costs that had been sent to the defendant within the meaning of the English *Solicitors Act 1932.*[8] The bill of costs had been accompanied by a letter, at the end of which the plaintiff had applied a rubber stamp with a facsimile of a signature that read "Goodman, Monroe & Co" on it. The Court of Appeal held, by a 2-1 majority, that this was sufficient to meet the requirements of the 1932 Act, because the plaintiff himself had applied the rubber stamp with the facsimile of his firm's signature.

7.19 While in the specific circumstances the statutory requirements had been met, nonetheless the Court stated that it was undesirable that a stamp would be used to "sign" a document. Indeed, having examined the relevant case law as to "signing" under a number of statutory provisions, such as those already discussed in this Consultation Paper, and having regard to the ordinary meaning to be found in dictionaries, Lord Evershed MR stated that:[9]

---

6 (1874) LR 8 QB 305, at 307.

7 [1954] 1 QB 550; [1954] 1 All ER 763.

8 The comparable Irish legislation for the purposes of a bill of costs is the *Attorneys and Solicitors (Ireland) Act 1849* (12 & 13 Vict., c.53), as amended. The requirement that a bill of costs be "signed" is contained in O.99, r.18 of the *Rules of the Superior Courts 1986.*

9 [1954] 1 QB 550, at 555; [1954] 1 All ER 763, at 765.

> "the essential requirement of signing is the affixing, either by writing by pen or pencil or by otherwise impressing on the document one's name or "signature" so as personally to authenticate the document."

7.20 This is, of course, consistent with the general definition in *Stroud's Judicial Dictionary*[10] which Finnegan J later cited in *Dundalk AFC Interim Co Ltd v FAI National League*.[11]

7.21 Denning LJ dissented from the majority decision of the Court of Appeal, finding that using a rubber stamp did not comply with the requirements of the 1932 Act. He considered that a personal input was required to conform to the ordinary meaning of the word "signature." He stated:[12]

> "In modern English usage, when a document is required to be "signed" by someone, that means that he must write his name with his own hand on it.... If a man cannot write his own name, he can "sign" The virtue of a signature lies in the fact that that no two persons write exactly alike, and so carries on the face of it a guarantee that the person who signs has given his personal attention to the document. A rubber stamp carries with it no such guarantee, because it can be affixed by anyone. The affixing of it depends on the internal office arrangements, with which the recipient has nothing to do. This is such common knowledge that a "rubber stamp" is contemptuously used to denote the thoughtless impress of an automaton in contrast to the reasoned attention of a sensible person."

7.22 Although Denning LJ was in a minority in the *Goodman* case, his general views, and in particular the first sentence in the passage just quoted, were quoted with approval by the English Court of Appeal in *Firstpost Homes Ltd v Johnson*,[13] which involved the sale of land. In the *Firstpost Homes* case, the Court held that merely typing a person's name on a document was clearly not a "signature" and did not constitute "signing" for the purposes of the English equivalent of section 51 of the *Land and Conveyancing Law Reform Act 2009*, discussed above.

7.23 In view of this case law, the Commission notes that, as a general rule, it is correct to say that a "signature" ordinarily requires a person to write his

---

10 Indeed, the *Goodman* case is also cited in *Stroud* as to what is a sufficient signature in the specific context of a bill of costs: *Stroud's Judicial Dictionary of Words and Phrases* 6th ed (Sweet & Maxwell, 2000), Vol 3, p 2453.

11 [2001] 1 IR 434, discussed above.

12 [1954] 1 QB 550, at 561; [1954] 1 All ER 763, at 768.

13 [1995] 4 All ER 355.

or her name with his or her hand on a document. There may, of course, be situations, such as those in the *Dundalk AFC* case, where a person can authorise another person to sign or his or her behalf and that this will also constitute a valid "signature." This form of signature by an agent is also useful in the context of corporate signing, where a name – or a company seal – may be affixed by an authorised officer of the company, such as a company secretary. In the context of digital signatures, the Commission returns later in this chapter to the important issue of digital signatures which are "affixed" by the person themselves or by an authorised third party.

7.24 The Commission provisionally recommends that, in general, a "signature" should be defined as "a writing, or otherwise affixing, of a person's name, or a mark to represent his name, by himself or herself, or by his or her authority with the intention of authenticating a document as being that of, or as binding on, the person whose name or mark is so written or affixed."

B Emergence of Digital Signatures

7.25 As the Commission discusses below, legislation such as the *Electronic Commerce Act 2000* has built on the long-standing common law rules as to what constitutes a "signature" in setting out tests to verify and authenticate electronic documents. As the Commission discusses in detail below, electronic, or digital, signatures, come in different forms, but the essential distinction is between a basic or light digital signature and an advanced digital signature. An advanced digital signature involves a unique form of individualised identifier based on some form of certification. The Commission notes that the more recent legislative frameworks on electronic signatures have moved towards requiring secure certification technologies which employ advanced electronic signatures. These have been used for many years in, for example, Canada and the United States and this approach was also adopted in the 1999 EU Electronic Signatures Directive,[14] which was implemented in Irish law in the *Electronic Commerce Act 2000*.

7.26 Two principal approaches have emerged in consideration of the reliability of electronic documents to ensure their acceptance as evidence in legal proceedings. The first is to indicate only the general nature of the results to be achieved in using electronic and automated documents, leaving the details to be determined by the parties. The second is to spell out in detail the technology or at least how the technology is to work to create legal effects. Both approaches have been tried in electronic signature legislation, and indeed some legislation represents a combination of both for different kinds of signature.

---

[14] Directive 1999/93/EC.

(1) How digital signatures differ from traditional signatures

7.27 The act of signing has been described as a "fundamentally legal act."[15] As already discussed in the context of signatures in the context of traditional documents, the circumstances may indicate that certain requirements or formalities ought to be observed which may have the effect of prescribing the style of signature to be used. This may be based on the security it provides or other characteristics suitable to a particular transaction. The primary rationale for introducing any signature requirement into either a traditional or a digital document is to ensure that any subsequent document purporting to be the original can, if necessary, be easily shown to be a fraud. The process of generating electronic or automated documents and signing them in this way is a means by which to attribute real life characteristics to a computationally derived document but the technologies involved mean that most users think of such documents as being particularly susceptible to undetectable fraudulent alteration and amendment. Electronic signing in the form of e-signatures is therefore a means to ensure that electronic documentary records are appropriately secure.[16]

7.28 This kind of advanced signature has a strong juridical value in that it provides a warranty for the authentication, confidentiality and integrity of the signature received as having been the same as in the text sent and assures that no modifications have been made.[17] Where a signature is uniquely associated with an identifiable or specified individual or undertaking this provides for non-repudiation of transactions where the sender cannot say that he did not dispatch the digital document in question and nor can the recipient claim that he did not receive it.

7.29 A widespread use of electronic signatures, which is not as yet the norm, would see a uniform and coherent means of verification. This could take the place of the myriad arrangements currently in use and would therefore contribute to commercial certainty. This would, the Commission notes, benefit both private sector commercial activity and also the State, which is a major agent of commercial activity.

---

15 Reed, "*What is a signature?"* (2000) 3 The Journal of Information, Law and Technology http://elj.warwick.ac.uk/jilt/00-3/reed.html/.

16 Wright, "*Eggs in baskets: distributing the risks of electronic signatures*", 15 J. Marshall Journal of Computer & Information Law 189 (1997).

17 This is made possible where modifications can be observed by referencing the hash function and message digest (components of PKI to be discussed below).

(2) The increasing need to provide a legal framework for electronic signatures

7.30 With technology becoming the norm and commercial documents becoming increasingly reliant on electronic technologies for speedy and cheap dispersal, it is becoming necessary to make formal legal provision for the admissibility of electronic signatures in legal proceedings to validate electronic documents in evidence.

7.31 Transacting over the internet poses particular problems and as a forum it is uniquely open to fraudulent or communication through pseudonyms under acquired or fabricated identities. The issue of proving the identity of a party engaged in an on-line transaction arose in just these circumstances in a 2002 case in Germany. The facts were concerned with a contract to purchase a watch through an internet sale auction.[18] An offer of €9,000 was received from the defendant's email account which was pass-word protected. When the seller sought payment the defendant refused and denied making the offer claiming that any offer made had been made by an unauthorised third party. It must be pointed out that prior to the "offer" having been made, the defendant had become aware that his email account and password had been compromised and indeed the service provider had blocked his email account. It was held by the Higher Regional Court of Cologne that the use of the email account alone was insufficient to meet the onus placed upon the plaintiff to show that the defendant had made the offer. It was suggested that the use of an electronic signature could establish *prima facie* evidence that the sender was the signatory which would in effect reverse the burden of proof.[19]

7.32 In the absence of a specific statutory requirement to the contrary, there is no requirement that any document be signed as a prerequisite to legal validity. Yet there are many statutory requirements for signatures (usually coupled with a requirement that the instrument be in writing) a prominent example of which can be seen in section 2 of the *Statute of Frauds (Ireland) 1695*. Thus while it is unusual for the legislative provision to define what is a "signature" or what constitutes "signing", (there is no such definition in Irish legislation), a large proportion of commercial documentation is signed even with no strict legal necessity.

7.33 Documents are not an immutable means of communication. Given the ease with which documents, be they traditionally executed hard-copy documents or electronic and automated documents can be altered it is

---

[18] *Case No. 19 U 16/02*, Oberlandesgericht Koln, September 6, 2002.

[19] A similar approach was approved in the Regional Court of Konstanz in *Case No. 2 o 141/01.*

necessary to identify a reliable means by which to establish whether the evidence has been tampered with. This is essential in both civil and criminal cases. As regards furnishing electronic and automated documentary evidence this usually involves the use of file interrogation procedures often called electronic forensics and which tend to focus on establishing a verifiable chain of custody.

7.34 A further justification for imposing regulation on the system of signatures for use on digital documentation stems from the view of electronic signatures as different from those signatures on paper. A manually executed signature on paper involves two parties in the ceremonial act of signing. While an electronic signature may also involve the same classes of parties, ie the signer and the relying party, it may also involve a third person, someone who acts as an intermediary to establish the relying party's identity is an attempt to create trust in the signature itself as a fact. This trusted third party is authorised to certify to the relying party that the signature bits which make up an e-signature are in fact the signature of a particular person. This provides stability and confidence in the transaction.

7.35 In consequence to the position of trust they occupy, the legislation has thus been devised to ensure that such certification authorities (CAs) follow certain procedures. Certification Authorities are usually permitted to limit their liability for mistakes of identity where the proper procedures have been followed. Others offer the relying party reinforced credibility of the identification in such certificates by way of a presumption of attribution.[20]

7.36 The Australian case of *Clipper Maritime Ltd v Shirlstar Container Transport Ltd (The Anemone)*[21] held that a printed name sent by telex is sufficient, where Staughton J noted obiter that, as far as section 4 of the *Statute of Frauds 1677*[22] applied "the answerback of the sender of the telex would constitute a signature, whilst that of the receiver would not since it only authenticates the document and does not convey approval of the contents".

7.37 The issue of e-signatures does not create a new legal conundrum. In essence it remains focused on the essential functions of any signature. It must be held in mind that the issue of documentary authentication and attribution is

---

20 When such signatures are created by asymmetric or public-key cryptography, they are called digital signatures, and the system of hardware, software and rules that govern the signature, certification and reliance processes is a public key infrastructure (PKI).

21 [1987] 1 Lloyd's Rep 546.

22 The equivalent of the *Statute of Frauds (Ireland) 1695*.

not purely one of law and there remains a distinction between basic legal requirements and prudent business practices.

7.38 Any legislative reform should attempt to be completely media-neutral and dictate how the basic principles of evidence can be met by intangible information.This is done by addressing the authenticity and admissibility of the electronically or automated document as a primary concern of the *Evidence Bill*.

7.39 The *Electronic Commerce Act 2000* represents a competent, if uneven application of these principles. E-Signatures are just one form of evidence of attribution in this statute. In effect this law maintains the link between traditional and electronic signature vocabularies and allows certification technologies to create a signature but leaves the essence of a signature in law the same as it was for a signature on paper.

7.40 The elements of reliability of attribution of a document are many, and the technical aspects of the signature, on paper or electronically executed, are only part of the "threat/risk analysis" undertaken.

(3) The Volatility of Electronic Documents

7.41 When presented with electronic commercial documents, evidential concerns focus on ensuring that these records are what they purport to be, that they are complete and have not been altered. These challenges are addressed by examining the documents in terms of their authenticity and integrity.

7.42 How then do the requirements and concepts of authenticity and integrity functionally apply and what can be done to ensure the stability of these digital objects or the systems that maintain them? Much of the information concerned which will be later reproduced in (tangible) legible form (most commonly a printout) is available in digital form only and therefore has no standing physical representation. Word and XML documents may be created from original input. It is essential that a commercial document which is continually in flux can be archived, frozen and extracted for evidential purposes even where the parties involved have no history of transacting with each other. This is particularly of relevance in high-end commercial transactions such as property transfers. For instance in the absence of a centralised securely maintained register there is no means by which to electronically search to establish the status of the title held over any property which may be the subject of a land transaction. Such a system would mean that when it comes to buying and selling property the planning process and the good title of the alleged owner can be effectively and electronically tracked and traced.

(4) The Birth and Evolution of the Electronic Signature

7.43 When the first contract was signed and faxed it created the basis for the discussion of electronic signature validity. After all it was the first time

someone could sign something, place it in a machine, send it from one phone line to another and deliver a digitally reproduced signature. The path this signature took was not controllable or traceable, but nonetheless the issue as to whether it constituted a valid signature could be determined on an analysis of basic principles. Thus, the intentions of the signature were clear. Following a succession of decisions in which courts on different countries ruled that this method of signature capture carried the same validity as if the parties were standing in the room together, the fax became a standard procedure for concluding contracts world-wide.

7.44 Problems however arose in the so called "fading fax" cases where the franks and ink used on early faxing cartridges degraded. The original fax paper's ink would vanish after a period of time (the paper was not thermal-treated) which involved making a copy on a photocopier to make the information on the fax suitable for permanent storage. The quality of these images was often poor or barely legible, but businesses understood the intention and would consider it signed even if there was only a partially legible signature. So in essence this was a copy of a copy (a derivative) of a digital image, and even with the potential for alteration, the fax remained admissible.

7.45 From a commercial stand point, prior to the introduction of fax machines, many contracts would have been conducted in a face to face bargain, reduced to a document which could then form documentary evidence of the transaction. Therefore prior to any foundation requirements, electronically executed commerce operated on a system of trust. The Commission now turns to consider why did the development of the electronic signature means that courts now place so much reliance on this means of signing for legal certainty.

7.46 In the English case *Re a Debtor (No. 2021 of 1995),*[23] the form of signature was examined. The case centred on a proxy form for a creditors' meeting under section 257 of the *Insolvency Act 1986* and which had been faxed to the chairman of the meeting. Rule 8.2(3) of the English *Insolvency Rules 1986* stated that the form was to be "signed by the principal, or by some person authorised by him". Crucially it was conceded in the case that the act of signing could not be viewed strictly so as to be limited to "the narrow concept of marking a substrate manually by direct use of a pen or similar writing instrument" and that the form could in fact be "signed" by means of a stamp. This is rather akin to the approach taken in *Goodman v J Eban Ltd.*[24]

7.47 In *Re a Debtor (No. 2021 of 1995)* it was held that the form was in fact signed sufficiently within the meaning of the Rule and that the concessions

---

23 See [1996] 2 All ER 345.

24 [1954] 1 QB 550; [1954] 1 All ER 763. See paragraph 7.18 above.

as to stamping were valid, as even a requirement for direct manual signing could not guarantee the authenticity of the document. Laddie J stated:

> "[T]he function of a signature is to indicate, but not necessarily prove, that the document has been considered personally by the creditor and is approved of by him... Once it is accepted that the close physical linkage of hand, pen and paper is not necessary for the form to be signed, it is difficult to see why some forms of human agency for impressing the mark on the paper should be acceptable while others are not.
>
> For example, it is possible to instruct a printing machine to print a signature sent by an electronic signal sent over a network or by a modem. Similarly, it is now possible with personal computer equipment…to compose say a letter on a screen, incorporate within it the author's signature which has been scanned onto the computer and is stored in electronic form, and to send the whole document including the signature by fax modem to a remote fax. The fax received at the remote station may well be the only hard copy of the document. It seems to me that such a document has been 'signed' by the author."

7.48 This general approach is also consistent with the case law on signatures involving traditional documents, already discussed. The Commission notes, in this respect, that the advent of the fax did not pose "new" issues as far as determining what constituted a signature, but merely the application of existing approach and rules in a new setting.

(5) Specific issues in the context of en electronic-signature

7.49 The Commission notes that an electronic signature is a form of a computer-based personal identity. As such it is a form of identification analogous to a hand-executed signature written on a paper document. These can be in the form of a simple scanned image of a handwritten signature on a tactile record, which is known as a bitmap signature. They can be a more technologically advanced form of signing uniquely tailored for the document at hand such as the e-signature. This popular type of the digital signature is founded on public key cryptography.[25]

---

[25] Throughout this chapter reference will be made to both 'Public Key Cryptography' and 'Public Key Infrastructure (PKI)'. Public key cryptography is the most common method on the Internet for authenticating a message sender or encrypting a message. The public key infrastructure assumes the use of this cryptography to establish the system creating and sharing a pair of keys for the encryption and decryption of messages. Unless control of the private key is lost or

7.50 The basic characteristic of this secure encryption technology is that two different but mathematically related keys, the private and the public key (the so called "key pair"), are used in order to create a digital signature and encode the data and to verify the signature and decode the data. Electronic signatures represent a means and method of verification of the sender's identity and when adduced in evidence can attest to this.

7.51 The internet has been cited as an unsafe and unregulated medium through which to do business.[26] Documents exchanged through internet or electronics-based matrixes have only been academically considered sufficiently verifiable to enable anything more than a "use at your own risk" approach to e-commerce.[27]

7.52 In general the common law does not give signatures or signed documents any special status as evidence, except for documents signed by public officials which may be self-authenticating and admitted without proof beyond that of the signature. The basic function of a signature be it a traditionally hand executed method of witnessing or an electronic version, is to link a person with a text or document. The signature may be made by the person or by someone acting for that person by proxy.

7.53 The idea of a signature is broad and not specifically defined. But the question of whether a document is "signed" remains essentially a question of fact. Understood in this way, electronic signature legislation which regulates the area is merely to assure that the signature may be accomplished through electronic means.

(a) Integrity

7.54 For evidential purposes how is the integrity of an electronic signature which will certainly bolster the likelihood of having a document admitted as evidence, to be tested? Testing the integrity of an electronic signature requires

---

compromised, it is statistically impossible even for a computer to deduce the identity of the private key from the public version. (R. Jason Richards, "*The Utah Digital Signature Act as 'Model' Legislation: A Critical Analysis*", 1999, 17 J. Marshall Journal of Computer and Information Law, 873, 880-81.) The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.

[26] Cross, "*BT Trustwise- Enabling eCommerce Through Trust*", 1999 BT Technology Journal, Vol 17 (3) 44-49.

[27] Labuschagne and Eloff, "*Electronic Commerce: The Information Security Challenge*", Information Management and Computer Security, 8 (3), 154-157.

establishing a reasonable belief that any file electronically signed on a system cannot be and has not been tampered with by anyone or anything.

7.55 In the context of a traditional hard document, the possibility for visual examination means that any discrepancies may be detected, but with electronic records it can be difficult to manually or even visually tell if the file has been altered.

7.56 It is therefore arguable that an electronic signature sufficiently qualifies as a signature without any legislative assistance as it is capable of identifying or facilitating the identification of a person where linked to a text. There is, therefore, a need to legislate for electronic signatures to provide certainty for signatures which are an important symbolic part of a transaction and to ensure that this means of witnessing would be legally acceptable in spite of their relative novelty.

7.57 Legislative regulation is, therefore, a means by which to set out the duties of parties to electronic signatures in a manner intended to reduce any perceived risks associated with them as a means of signing and also to promote electronic commerce.

C Differing Technologies and Legislative Frameworks for Digital Verification

7.58 In this Part, the Commission turns to discuss the varying forms of technology and legislative frameworks that have developed in different States to authenticate and verify digital signatures.

(1) Electronic Signature Technologies Explained

7.59 Authentication in the context of electronic documentary evidence may focus on either entity authentication or data origin authentication. Passwords have until recently provided the mainstay of identity for entity authentication since multi-user information systems came into being. Ford and Baum have highlighted the unsuitability of this insecure technique for safeguarding information and note that it "constitute(s) one of the major vulnerabilities of electronic commerce systems" given the hazards of external disclosure, cyber-eavesdropping and manual guessing leading to infiltration of electronic systems.[28]

7.60 Security passwords are often combined with physical tokens, for example, account numbers are stored in the magnetic strip of a credit card used in combination with a pin number password to ensure identity and protect

---

[28] Ford and Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption ,* 1997, Prentice Hall Inc,. New Jersey.

access to funds. Tamperproof universal integrated circuit cards are being developed and are a type of advanced smart card using microprocessor memory. These can contain up to 80 times the memory capacity of a traditional memory card and can be used as an identification card or to make secure financial transactions or to hold electronic signatures.

(2) Digital Signatures v Electronic Signatures

7.61 Although the terminologies are used interchangeably, digital signatures are a subset of electronic signatures. There are marked differences between digital signatures and other forms of electronic signatures. Digital signature technology serves a more specialised market than plain electronic signatures and has its own legal questions associated with it. A digital signature is not a signature in the traditional sense. It is based on a strictly regulated exchange of digital number combinations and therefore requires that the user has both a card reader with the relevant software and a chip card. This card contains the "private key", which is a code made up of a combination of numbers. A person ordering goods or transferring money over the internet signs using his private key, which is protected by a PIN (personal identification number). The recipient of the data verifies the digital signature with the sender's "public key" and thereby confirms that the information is genuine. This rather simplistic explanation is expanded more fully below. A public key has been described as "a surrogate presence in cyberspace for some entity in physical space. It acts directly in cyberspace, just as the associated entity can act in physical space."[29]

7.62 The dominant electronic signature technology in use is based on a formula established in the 1970s when "public key" encryptive technologies developed. Public Key Cryptography is based on the premise of two separate but dependent keys operating in sync with one digital signature encrypting the data message and another being used to decrypt and legitimate it. The originating starting-point key is, being public, just that. It is accessible to the public at large while its private counterfoil is withheld from the public forum by its holder.

7.63 PKI operates a linear structure and can be best explained as follows. While distinct in their own right the two keys are mathematically inter-related and dependent on each other to function. The public key cannot be legitimated by any but its private equivalent. It is therefore impossible to deduce the identity of the private key from the publically available information.

---

[29] Ellison, "*Establishing Identity without Certification Policies*", 1996 available at www.clark.net/pub/cme/usenix.html.

7.64 This aids in the authentication of digital "documentary" objects. The recipient's task is to decipher the message digest and to verify the sender of the message. This is not straightforward and the difficulty remains in that it must be assumed that the public key is correctly associated with the sender in that he has retained control of his key and has not allowed this to be compromised. A recipient's ability to verify the integrity of the message is done by means of his creating his own message digest and comparing this to the supposed sender's deciphered message digest. Should the two message digests accord with each other, the integrity of the message is vouchsafed.

7.65 In their operation, digital signatory devices employ a merged PKI and hash function. "Hashing" refers to the process of creating a string of characters, also called a digest through mapping from the full plain-text message (this is done through the use of an algorithm) and the combination of these serves to compress rather than manipulate the data into a single unique message digest. Should any alteration to the material in a digitally signed document take place, the digest also mutates and changes become detectable.

7.66 Digital signatures involve particular steps which can be illustrated as follows. Party A wishes to create a digital signature to securely transact/correspond with party B. Party A first creates a message digest for the document which he then encrypts with his private key. Party A then transmits the encrypted message digest and the digital document to the recipient (party B). Party B then uses the sender's publically available key to decode the message digest which interlocks with the private key issued to him by the sender.

7.67 The issue which arises focuses on the means, if any, by which to guarantee that the holder of the private key is representative of the person purporting to hold it. A solution to this problem is to employ the use of a third party whose status is above reproach to vouch for the signature. This third party, who has no other involvement or stake in the transaction, certifies that a given party to the transaction is associated with a given public key and correspondingly holds the private key. This position is usually the preserve of a certification authority.

(3) The Benefit of Advanced Electronic Signatures

7.68 Electronic signatures executed by means of signing premised on PKI are secure to the extent that they are based on a system of asymmetric cryptography (PKI) which ensures a high level of security in e-communications and of confidentiality in the context of a message sent over an open network such as the Internet.

7.69 The protection afforded by advanced electronic signatures is sufficient to safeguard e-transactions, offer security and transparency and afford

sufficient evidential rigour to enable the authentication and eventual admissibility as evidence of documentary contracts concluded in this manner.

7.70 Electronic signatures also significantly strengthen the authentication of the identity of the signer by attributing the message to him through the unique characteristics of the key pair which brings finality of both form and parties to the transaction. Electronic signatures cannot easily be forged, unless the signer loses control of his private key.

7.71 Even though these functions of electronic signatures can guarantee security over open networks and strengthen consumer trust in e-commerce, another challenge concerning the identification of the parties remains. This relates to the question of establishing the personality of those who are engaging in electronic commerce. How can it be proved who participated in a particular transaction so as to prevent repudiation of the transaction? In other words, how secure is the security provided by electronic signatures if such a means were to be adopted as a uniform method of verifying the integrity of documentary evidence to bolster its admissibility?

(4) Development and Implementation of Electronic Signature Technologies Internationally

7.72 Although electronic signatures came to prominence in the 1970s, many jurisdictions were slow to adopt a legislative regime to regulate them. Motivated by necessity, the late 1990s saw the emergence of much legislation. Most of these initiatives were based on the prescriptive model, with PKI as the technology of choice employed. The process began in the United States, and many subsequent legislative regimes reflect the influence of the *Utah Digital Signature Act 1995.*

7.73 The use of PKI technology and its incorporation into our domestic law through the *Electronic Commerce Act 2000* lays down a framework for the provision of evidential certainty in relation to electronic signatures. It regulates the authenticity of the document through a process whereby the party who signs can be identified as the source or origin of the signature. It also copper fastens the integrity of the communication which is concerned with the accuracy and completeness of the document. From a contractual perspective the use of PKI aims to ensure that a signatory to a document cannot repudiate it in the event of a dispute. It also ensures confidentiality, as the communication can be kept as a matter between the parties.

7.74 As a proponent of relevant US federal E-Sign legislation, Senator Spencer Abraham suggested that e-signature legislative provisions “literally

supply the pavement for the e-commerce lane of the information superhighway."[30]

(5) The legal functions of electronic signatures and technologies involved

7.75 Electronic signatures must conform to the same functionary requirements as their handwritten equivalents namely:

(i) Authentication

(ii) Integrity and

(iii) Non-Repudiation

7.76 It must be noted that the emphasis in authentication in these circumstances is focused on ensuring that a party to a transaction is the person reportedly represented in the transaction. Assuring the integrity of an e-signature confirms that a communication has not been altered at any point during transmission from the source to the intended end-recipient.

(6) Different models of electronic signature legislation

7.77 Fischer identifies a troubling lack of uniformity amongst the disparate international e-signature legislative provisions which she sees as a "dearth of technological standards for e-signatures."[31] This is puzzling given the overall shared aim of bestowing legitimacy upon electronic signatures and the attempts to equalise these signatures with their hard-copy, handwritten counterparts. The lack of any degree of synranicity on how best to achieve this goal has resulted in what one commentator has termed a "veritable Tower of Babel".[32]

7.78 Although they reflect different assumptions on the legal status of electronic signatures, they can be classified into three categories. There are three legislative models which have come to the fore and which have been agreed upon and embodied in legislative frameworks for the regulation of electronic signatures and are now explained.

---

30 Statement of Sen. Abraham, 146 CONG. REC. S 5223 (daily ed. June 15, 2000), library of Congress. Available at Thomas.loc.gov/cgi-bin/query.

31 Fischer, "*Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation",* Association of American Law Schools 2001, Annual Meeting: Section on Law and Computers.

32 Aalberts and Van der Hof, *"Digital Signature Blindness: Analysis of Legislative Approaches Towards Electronic Authentication",* § 1.2, 7 The EDI Law Review 1-55, 2000.

- **The Mandatory Approach**

7.79 The mandatory approach is also called the prescriptive model. It is technologically specific and effectively mandates an identifiable means of sealing an electronic document. This is to be achieved through the use of digital signatures based on public key cryptography technology.

- **The Minimalist Approach**

7.80 The minimalist approach is a method of regulation which is technologically neutral and does not mandate an electronic format for recognising e-signatures.

- **The Hybrid Model**

7.81 The hybrid model is expressed in terms of technological neutrality but this approach still invests some signatures with preferential status and legal presumptions of validity.

(a) The Mandatory/Prescriptive Model

7.82 This approach is rooted in the concept that PKI is the only sufficiently tested technology to adequately safeguard e-commercial transactions. Boss comments that the rationale for this stems from the proponents of "prescriptive legislation contend(ing) that legal certainty is key to stimulating widespread public trust in electronic signatures."[33]

7.83 A feature of this prescriptive or mandatory model which recommends it is that its use promotes and serves to establish a definite legislative framework for prescribing the obligations and liabilities of the parties to a given electronic transaction. This necessarily entails laying out the liabilities of the certification authorities.

7.84 A different result can be achieved by legislatively delimiting the liability of certification authorities, although this has the effect of exposing consumers to greater risk and uncertainties. This could slow the up-take of e-signatures and thus serve to undermine the aim of the legislation where the primary goal is uniformity, equality of regulation and consumer protection.

7.85 A clear example of this legislative approach can be seen in the Malaysian Digital Signature Act 1997 which provides that a certification authority will bear no liability except where it elects to waive the protection for any loss incurred where a party relies on a "false or forged digital signature" where the licensed authority has complied with the requirements of the Act. In such circumstances the subscriber bears unlimited liability for any loss incurred

---

[33] Boss, "*The Internet and the Law: Searching for Security in the Law of Electric Commerce*", 23 Nova Law Review 1999, 583 at 598.

or damage sustained through fraud, or the loss of a signature of which he may have been unaware. While this may serve to protect certification authorities from liability in instances where they could not foresee or prevent such harm, and enable them to operate at a commercial level, this does not impose any kind of watch-dog obligation on them to stay abreast of the legitimacy or otherwise of their clients' business interests which they are essentially guaranteeing to another party.

(7) US Technology-Specific Legislation- the Utah Digital Signature Act 1995

7.86 The first US legislation containing provisions for public key cryptography as a means of signing was the *Utah Digital Signature Act 1995*. It regulated certification authorities and exempted them from liability if they followed certain specified rules. It also provided a presumption of attribution for duly certified signatures.[34]

7.87 As a first generation piece of legislation the means of regulation it prescribed was heavily criticised as distorting the real value of the technology to legislate liability. Gregory noted that "(e)ssentially the statutes were allocating risk by law differently than how the real risk fell"[35] and that this amounted to "legislating market winners", a course which was inappropriate in a free market.[36]

7.88 The Utah legislation was seen as too static and unyielding to emergent technologies. It did not take account of the different means of executing and implementing a digital signature which carry different degrees of involvement by certification authorities and thus distribute risk differently.

7.89 Finally, from a development perspective, the Utah provisions were in danger of impeding the development of more nuanced signature technology, as they gave an unfair legal advantage to the vocabulary of public key cryptography. The above criticisms mean that no further states have followed the Utah model.

7.90 The mandatory/prescriptive approach does not allow sufficient breathing space for market forces and can be seen as over-protecting certain

---

[34] Utah Act, Utah Code Annotated, Title 46-3, http://www.le.state.ut.us/~code/TITLE46/46_02.htm. The Utah example was followed by three other states; Washington, Minnesota and Missouri.

[35] Gregory, JD, "*Authentication Rules and Electronic Records*" Ontario, Canada Canadian Bar Review, November 2001. Available at www.cba.org.

[36] Biddle, "Legislating Market Winners" (1997), available athttp://www.acusd.edu/~biddle/LMW.htm.

sectional interests and technologies at the expense of innovation which may amount to an exercise in government regulation of the markets.

(8) The Hybrid Model

7.91 The hybrid model represents a shift towards a more market-driven legislative framework for the regulation of digitally-based transactive commerce. This model is heavily influenced by the UN Commission on International Trade Law's Model Law on Electronic Commerce (MLEC) enacted in 1996 and which is aimed at facilitating the use of modern means of communications and methods of storing information. It is based on the aim of establishing functional equivalence as between electronic media and true paper-based concepts such as "writing", "signature" and "original". This model adopts a pseudo-technologically neutral stance while displaying no ideological preference for any particular electronic programmes or mechanisms.

7.92 The hybrid approach was adopted by a number of jurisdictions including Singapore (*Electronic Transactions Act 1998*) and Bermuda (*Electronic Transactions Act 1999*). More importantly, this two-tiered model was also adopted in the1999 EU Electronic Signatures Directive, which is discussed below.

(a) The UNCITRAL Model Law on Electronic Signatures- Hybrid Legislation

7.93 Adopted by UNCITRAL on 5 July 2001, the Model Law on Electronic Signatures[37] aims at bringing additional legal certainty to the use of electronic signatures and allows the parties to a transaction to determine in advance whether the reliability standard of the 1996 Model Law has been met. Building on the flexible principle contained in article 7 of the UNCITRAL Model Law on Electronic Commerce, it establishes criteria of technical reliability to ensure equivalence as between electronic and hand-written signatures while avoiding detailed descriptions of the technology to be used to achieve this. Earlier drafts talked of "secure" or "enhanced" electronic signatures. These terms have been dropped from the end result but the criteria of identification, sole control and detection of alteration remain in the new criteria for reliability of an electronic signature.[38]

7.94 The UNCITRAL Model Law on Electronic Signatures, which adopted the two-tiered approach, promotes the progressive harmonisation and unification of policies on e-signature issues including evidential issues and

---

37 Model Law on Electronic Signatures, 2001: <http://www.uncitral.org.

38 UNCITRAL Model Law on Electronic Signatures, art 6.

authentication[39] and the resulting matters of admissibility. It promotes functional equivalency with tangible documentary signatures[40] but shies away from the provision of a clear definition of digital signatures. The market forces driving this Model Law are not ignored and are recognised under Article 5. Articles 8-11 outline the liabilities of Certification Service Providers, signatories and relying parties and the overall orientation of the Model Law is to establish a reliable and fair global authentication system for electronic verification tools. Furthermore, the Model Law provides that the legal efficacy of foreign certificates and e-signatures in the Member States depends on their level of reliability, which is determined either by international standards or by the contractual agreement between the parties.

7.95 However, far from embracing an endless suite of differing digital means of securing e-transactions, the hybrid formulation is founded on a policy of limited technological neutrality. This is exemplified by the 1999 EU Electronic Signatures Directive,[41] the central tenet of which is the achievement of functional equivalency between electronic signatures affixed to a digital document and their logical counterparts on physical hard-documentation. Consequently digital signatures are not to be denied legal legitimacy or admissibility stemming from their mechanical origin.

7.96 Despite the technical neutrality anticipated in a directive of this sort, there is a level of technological favouritism woven into the Directive. This includes the presumptive distinction for the purposes of authentication bestowed upon electronic signatures executed and verified by means of a qualified signature complying with certain restrictions.[42] The technological favouritism here can be identified in the structure laid down for the creation of these qualified signatures which are accorded a higher level of trust as "advanced electronic signatures" where created using a secure-signature-creation device and affiliated with a qualified certificate.[43] While the Directive stops short of mandating their creation by a particular process, it remains the case that there is, as yet, a singular technology which is capable of fulfilling the requirements set out in article 5 and this is PKI. It therefore follows that PKI

---

39 Article 6(3).

40 Article 6(1,2) provides that when a document is digitally signed, it is as legally valid as a hand-written signed document.

41 Directive 1999/93 EC, OJ L013, 19/1/2000, p 0012-0020, available at www.europa.eu.int.

42 Article 5 (1)(a) and (b).

43 Explanatory memo point (20).

remains the defining means of producing electronic signatures to satisfy a hybrid regulatory regime.

(b) The Advantages of the Hybrid Model

7.97 The objective of this "hybrid" method, which is adopted by the EU, is the provision of "time-resistant regulations by setting requirements for e-authentication methods with a certain minimum legal power (a minimalist approach) and by attributing greater legal effect to certain widely used techniques (digital signature approach)."[44] Regulatory frameworks adopting the hybrid formulae are viewed as more flexible and adaptable to technological developments without the need for continuous amendment. It is therefore more fluidic and ensures a greater level of legal certainty which is necessary to bolster public trust in electronic signatures.

(c) Disadvantages of the Hybrid Model

7.98 The Model Law might at first seem limited in its application given that it applies only to commercial settings rather than to non-commercial civil or criminal matters. However Article 1 of the Model Law permits countries to extend the scope of the Model Law "beyond the commercial sphere" and therefore extend its remit beyond purely commercial disputes.

7.99 This approach also recognises a more innovative legal environment by ratifying the freedom of choice regarding authentication systems and allows discretion to States to implement international policies based on domestic concerns. However this can also be seen as a disadvantage which could limit the uniform recognition and the interoperability of e-signatures and electronic documents with negative connotations for the e-market.

(d) American Hybrid Legislation

7.100 As the Utah model fell from use, legislative attempts were made to find technology-neutral statutes which recognised the greater reliability of some forms of e-signatures over others. Perhaps the most prominent example of these was the *Illinois Electronic Commerce and Security Act 1998*[45] which provided scope to allow the parties to designate an electronic signature as being sufficient to satisfy a legal signature requirement. In addition, particularly reliable e-signatures were described as "secure electronic signatures". These had certain characteristics first described in the United States by the National Institute of Science and Technology (NIST) in the early 1990s.

---

44 Spyrelli, C, "*Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication*", The Journal of Information, Law and Technology (JILT) 2002(2), P 6.

45 Section 10-110.

7.101 The UECA[46] is silent on evidential principals generally. The Uniform Law Conference has adopted a separate statute on electronic evidence, the *Uniform Electronic Evidence Act 1998*[47] but it says nothing about signatures. The UETA says only that evidence of a record or signature may not be excluded solely because it is in electronic form.[48]

(e) Canadian Hybrid Legislation

7.102 In Canada, the federal government has adopted its own form of hybrid statute- the *Personal Information Protection and Electronic Document Act 2000 (PIPEDA)*[49] with Part 2 dedicated to electronic documents.

7.103 Again these provisions apply the principle of functional equivalence through signature requirements to be satisfied electronically by use of an e-signature in such form which is to be prescribed by regulation.[50]

7.104 This legislative instrument also allows for a hierarchical scheme of secure electronic signature where granted by regulation.[51] For example, one can use a secure electronic signature to create a certificate signed by a minister or public official that is proof of a fact or admissible in evidence.[52] A secure electronic signature may serve as a seal, if the seal requirement has been designated under the Act.[53] Affidavits may be made electronically if both deponent and commissioner of the oath sign with a secure electronic signature.[54]

---

46 *Uniform Electronic Commerce Act 1999* is the Canadian law modelled on the UN Model e-commerce legislation.

47 Proceedings of the Uniform Law Conference of Canada 164, http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2.

48 Section 13.

49 S.C.2000 c.5, http://lois.justice.gc.ca/en/P-8.6/index.html.

50 Section 36.

51 As defined by section 31 a “secure electronic signature" means an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1). Such a signature is not more rigorously defined.

52 Section 36.

53 Section 39.

54 Section 44.

7.105 Unlike the *Illinois Electronic Commerce and Security Act of 1998*, the Canadian federal statute gives no choice about whether to use a secure electronic signature. To sign electronically and validly within the meaning of the provisions, parties must use the secure electronic signature.

7.106 The Canadian federal legislation amended the *Canada Evidence Act 1985*[55] to allow the creation by regulation of presumptions of the association of secure electronic signatures with persons, and of the integrity of information in documents where a secure electronic signature is used.[56] No such regulations have been made to date.

7.107 In Quebec Canada, an electronic signature is approved where made "by means of any process that meets the requirements of article 2827 of the Civil Code", which is part of Book VII of the Code on evidence. No special rule of admissibility is provided. The Quebec statute did amend one article of the Civil Code on the use of electronic documents as evidence[57] without mentioning signatures in particular.

(f) Contrast with the EU Directive on Electronic Signatures

By contrast, the EU Directive on Electronic Signatures provides that qualified electronic signatures must be admissible in evidence, and that other electronic signatures may not be denied admissibility on grounds of their electronic form or because they are not qualified in one element or another.[58] To the extent that documents are more readily admissible when signed, and that in practice courts are more difficult to satisfy with less than an advanced signature, compliance with the requirements for an advanced signature would be more important in European law than in comparative Canadian or American law.

(9) Minimalist Legislation

(a) Reasons for Minimalism

7.108 The underlying technology used to generate, transmit and store electronic records is subject to constant rapid change and an ever-present danger is that technologies and regulating frameworks based solely on these risk becoming obsolete shortly after implementation.

---

55 RSC 1985 c. C-5.

56 Section 31.4

57 Article 2837 is repealed and replaced by a new provision pursuant to section 77 of the information technology statute.

58 Directive 1999/93/EC Art 5 implemented in the *Electronic Commerce Act 2000.*

7.109 For this reason, any legislative reform or framework suggested ought to be based on the principle of "technological neutrality" to ensure the widest possible inclusion of electronic communications and documents which vary so widely that it would prove very difficult to introduce a single technological vocabulary to suit them all.[59]

(b) The Third Way; Minimalist Legislation

7.110 Criticism of the above prescriptive and hybrid models led to the evolution of a third legislative framework- the minimalist, market-orientated approach. Fischer notes that this model has flourished in market-driven climates and common law jurisdictions. Examples of the minimalist approach include the US *Uniform Electronic Commerce Act 1990* (UETA), the UK *Electronic Communications Act 2000*, Australia's *Electronic Transactions Act 1999* and New Zealand's *Electronic Transactions Act 2002*. The US adoption of the minimalist approach in the form of E-Sign can be seen as an attempt to reconcile and harmonise the disparate state regulatory regimes in use across the jurisdiction.

7.111 This species of legislation is entirely technologically neutral and fully attempts to integrate e-signatures and place them on a functionally equivalent par with their paper-based counterparts. No technological favouritism is displayed towards PKI or any style of digital verification instrument. Further to this, intermediary service providers are granted no special rights or obligations under minimalist legislation.[60]

7.112 It focuses on ensuring the reliability and enforceability of e-signatures and e-documents by removing existing legal obstacles from online commercial transactions and by establishing a technology-neutral status. Elements of the minimalist model are evident in the UNCITRAL Model Law on Electronic

---

59 "An Analysis of International Electronic and Digital Signature Implementation Initiatives", A Study Prepared for the Internet Law & Policy Forum (ILPF), September, 2000 available at http://www.ilpf.org/groups/analysis_IEDSII.htm.

60 The OECD Council Recommendation also adopted the minimalist approach as the UNCITRAL, with the intention to bolster confidence and promote the context of electronic authentication in information and communications infrastructures and to facilitate international e-trade by promoting cost-effective, interoperable and portable cryptographic systems. (OECD Guidelines for Cryptography Policy (1997) available at www.oecd.org.) These measures included Trust in cryptographic methods, choice of cryptographic methods, market driven development of cryptographic methods, technical standards for cryptographic methods developed at a national and international level, contractual or legislative liability of the Cryptography Service Providers (CSPs).

Commerce which deals with the functions of e-signatures and their binding power and recognises the full legal validity of digitally produced and signed documents (Article 7).[61]

7.113 The OECD Council Recommendation also adopted the minimalist approach as the UNCITRAL, with the intention to bolster confidence and promote electronic authentication in information and communication infrastructures and to facilitate international e-trade by fostering cost-effective, interoperable and portable cryptographic systems.

(c) Non-Uniform Minimalist Statutes

(i) E-Sign

7.114 Aside from the uniform statutes, both the US and Canada are home to a further example of technologically-neutral e-signature law. The American example is the federal statute, the *Electronic Signatures in Global and National Commerce Act*, known popularly as "E-Sign" dating from 2000,[62] an attempt to harmonise disparate interstate laws in the area of e-commerce and which was based on the Model Law and UETA.[63]

7.115 It aims to make the law almost completely media-neutral, and shows how standardisation in law can be achieved in electronic (and intangible) information. The stability of the content of the document is a primary concern of the Act.

7.116 In contrast to the 1999 EU Electronic Signatures Directive, this minimalist Act focuses on verifying the intent of the signatory rather than on developing guidelines. E-signatures, e-contracts and e-records are granted equivalent legal validity and enforceability with their corollary traditional forms and handwritten signatures.

---

61 Model Law on Electronic Commerce (1996) available at www.uncitral.org. The minimalist approach is also compatible with the ethos of the UN Model Law on Electronic Commerce and which is orientated towards minimalism in an effort to engage e-commerce usage on a global level with uniform minimalist regulation.

62 E-Sign, Public Law 106-229, June 30, 2000, can be found online at: http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=106_cong_public_laws&docid+f:publ229.106.pdf.

63 To prevent conflicting state level approaches, the law further prevents any individual state statute attempting to supersede E-SIGN in a manner that would discriminate for or against a particular technology. States may preserve or implement laws that offer an approach slightly different from that of the new federal law, but only where consistent with the overall terms of E-SIGN.

7.117 As far as the Act's interaction with a State's e-signature laws is concerned, it is provided in sections 101 and 102 that a State may pre-empt the Act only by adopting a 'clean' version of UETA as approved and signed by the NCCUSL[64] or by passing a technological-neutral law. The E-Sign Act thus establishes uniform and nationwide standards of acceptance, while taking into consideration the interest of the individual States. In terms of the international validity of e-signatures, the Act, consistent with the UNCITRAL Model Law on E-Commerce, removes paper-based obstacles to e-transactions and takes a non-discriminatory approach to e-signatures and authentication methods from other jurisdictions.

(d) The European Directive

7.118 Comparing the EU Directive with the US Act, the importance that the Act attributes, in practice, to the private sector and to self-regulatory policies is clear. The Act offers a legal framework for reliable and secure e-transactions and guards against any attempt at undue government involvement in e-commerce. In this vein, it refrains from setting up any mandatory scheme regarding e-signatures and certificates in favour of supporting a minimalist and interoperable legal platform for commerce. In essence the US legislation champions the same legal structure in the e-world that still protects the traditional manual commercial world. In support of the US system Spyrelli[65] notes that "political imperatives of catching cybercriminals and protecting consumers- connected with the fear of losing tax revenues online- push the EU to over-regulate and thus stifle the growth of e-business." However, the US approach, given the current state of authentication, may lead to consumers being put at risk, which in turn may lead to uncertainty surrounding the legal status of electronic signatures and of electronically signed electronic or automated documents.

7.119 Under the system in which the EU Directive and the implementing *Electronic Commerce Act 2000* function, the laws of evidence attribute full legal status to the handwritten signatures on paper documents when it comes to providing in court proof of any transaction. This means that under the Irish legislation where it is alleged that a computer's security has been compromised and that this has for example resulted in the forgery of an e-authorisation or in the modification of an e-document's content, the legitimate consumer is liable to prove that he was victimised by the fraudulent interference. It may be impossible in these circumstances for the user to prove the invalidity of a

---

64 National Conference of Commissioners on Uniform State Laws.

65 "*Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication*" JILT 2002 (2).

signature which is supported by a certificate issued by an accredited Certification Authority.

(i) Advantages of the Minimalist Model

7.120 Proponents argue that from a commercial standpoint the markets should influence the technologies chosen to regulate the area. This supports the contention that primacy should not be awarded to one particular technology. Any or several suitable technologies should be available where they most suit the task at hand.

(ii) Disadvantages of the Minimalist Model

7.121 Criticisms of this approach focus on the perceived vagueness of the minimalist framework. It is arguable that this could result in legal uncertainty, scupper the functional equivalency intended and detract from any attempts to establish PKI as a dominant uniform technology to regulate electronic signatures and provide authentic and admissible evidence should the need arise.

(10) Attribution of Documents and Signatures

7.122 The 1996 UN Model Law emphasises that presumptive attribution may be assigned where certain agreed security procedures are used in data messages. This allows the attribution of real life parties to these documentary instruments as to who caused them to be created.

7.123 Much like the unified concept of a document by which to define all traditional as well as electronic and automated documentary instruments, the Commission recommends a singular term “signature” to describe both manual signatures and electronic signatures but for the purposes of verification different definitions will be used for both.

7.124 The Commission provisionally recommends that a single term “signature” should be used to describe both manual signatures and electronic signatures but that for the purposes of verification, different definitions should be used for both.

(11) The Definition and Legal Effect of an E-Signature

7.125 NCCUSL attempted to follow the example of the UN Model Law but were unable to enact such a scheme following criticism based partly on the fluidity of the technology available and partly on the likely technological inexperience of its users. In the absence of legislative guidance on this matter, it is now the individual users as parties to the e-commercial activity who must satisfy themselves of the origin of electronic documents and signatures.

(a) The US Approach

7.126 The US in the 1990s witnessed the emergence of an amount of disparate legislation, varying from State to State in regulating the use of electronic signatures. Uniformity was desirable which led to the National Conference of Commissioners on Uniform State Law (NCCUSL) which published a *Uniform Electronic Transactions Act 1999* (the UETA). This was a comprehensive and authoritative national statement with broad national consensus on how electronic signatures should operate in a legal climate and was modelled on the UN Model Law on Electronic Commerce.

7.127 The UETA essentially means that a signature will not be denied legal effect purely on the basis that it is electronic in form. Following on from this a document will not fall where it bears an electronic signature and so will satisfy any writing or signing stipulations.

(i) Disparities with the EU Directive

7.128 The intention in the US and Canadian provisions is "to sign" and the means of endorsing the document is specifically phrased as "signing". Though the intention in the EU Directive on Electronic Signatures is the same its intent is couched in the language of "authenticate" rather than "sign".

7.129 None of the legislative provisions define the external appearance of an electronic signature. Therefore there is no requirement that the electronic signature look like a handwritten version when viewed. It is the intention to sign which is of fundamental importance and this can take the form of a code or symbol.

7.130 The UECA and the UETA provide that a signature requirement can be met by an electronic signature. The UN Model Law goes further in this respect and requires that an appropriate electronic signature must be as reliable as is appropriate in the circumstances.[66]

7.131 The US and Canadian Uniform Acts are not trying to legislate further, complex law. Their aim is to achieve neutrality as between traditional documentary and digital instruments and to make for better law.

7.132 The US Uniform Act though provides that where conditions are imposed by the signature service provider as regards apportioning or imposing

---

66 The EU Directive imposes no general requirement of reliability but leaves proof to the parties.

liability, the UECA[67] allows that authority to make a regulation imposing the reliability standards of the UN Model Law.[68]

7.133 At common law the execution of a signature on paper does not have to meet any test of reliability. If the association with a person is demonstrated and the intent to sign is demonstrated, the signature will be deemed sufficient.[69] The Commission recommends that e-signature standards should be developed uniformly, transparently and objectively and that the proposed legislative framework should give specific recognition to e-signatures that comply with any relevant international standards.

7.134 The Commission provisionally recommends that standards for electronic signatures should be developed uniformly, transparently and objectively and that the proposed legislative framework should give specific recognition to electronic signatures that comply with any relevant international standards.

7.135 This would also build towards a global consensus as envisaged by the UN Model Law on Electronic Commerce in an effort to encourage e-commerce with uniform minimalist regulation.

D The Current Climate for Electronic Signatures in Ireland and the EU

(1) The Electronic Signatures Directive 1999/93/EC

(a) The Use of Electronic Signatures

7.136 Legislative provisions incorporating these signatures focus on establishing a legal framework for the operation of digital signatures as well as incorporating formal requirements applicable in the offline transactions. In line with this approach any international regulations adopt PKI as the approved technology for generating e-signatures, imposing certain operational and financial requirements on Certification Authorities, prescribing the liability of key holders and defining the circumstances under which an electronic signature may be legally relied on where relief is sought through litigation.

7.137 The EU Electronic Signatures Directive was adopted in December 1999 and required Member States to comply with its provisions by July 2001. It

---

67 UECA section 10 (2).

68 The UETA has no such provision. E-SIGN permits states to enact such provisions only for limited purposes, generally in communications with the state government. E-SIGN section 104.

69 *R v Fredericton Housing* [1973] CTC 160 (FCTD).

represents one of a series of Directives, which together seek to put in place a legal framework for electronic communications, and e-commerce throughout the EU.

7.138 This was introduced in a climate of burgeoning growth in commercial transactions which are often conducted electronically with no complementary paper documentation. Removing the traditional mechanism by which the parties then identify themselves and validate the terms of the transaction resulted in the difficulty of ascertaining whether there was a sufficiently clear intention to enter into the transaction. This possibility of legal uncertainty over the legal effect of these electronic signatures represented a hurdle to the development of electronic commerce and the need for regulation in the area.[70]

7.139 As has already been outlined, this period saw the development by other jurisdictions of their own legislation to regulate the area.[71] This proliferation of national legislation represented a potential barrier to the internal market and prompted the need for uniform centralised regulation in the area.

7.140 Article 4.1 of the EU 1999 Electronic Signatures Directive states that its aims are:

> to facilitate the use of electronic signatures and contribute to their legal recognition; and
>
> to establish a legal framework for the electronic signature market by removing barriers to trade in the internal market.

7.141 The Directive ensures that signatures can be valid despite their electronic form and despite not meeting the more demanding standards described in the rest of the Directive. The outlook is phrased in terms of facilitating the use and recognition of electronic signatures. It is not prescriptive in its operation and grants a large level of discretion to Member States.

7.142 In seeking to give legal effect to electronic signatures, the Directive regulates two types of electronic signature. These are the electronic signature and the advanced electronic signature. The other type of advanced signature is also referred to as a digital signature. While often used interchangeably, a

---

70 See Commission Communication, A European Initiative in Electronic Commerce, COM (97) 157; Commission Communication, Ensuring Security and Trust in Electronic Communications: Towards a European Framework for Digital Signatures and Encryption, COM (97) 503.

71 Such countries included Germany Signaturgesetz, Bundesgesetzblatt, I, 1997, p1870 (1997), Italy (1997), Malaysia (1997) and Russia (1995). The US was the precursor to all these legislative regimes and many clearly reflect the influence of the Utah *Digital Signature Act dating from 1995*.

digital signature is distinguished from an electronic signature simpliciter as the former is generated as a result of applying specific technical processes to given information known as PKI.

7.143 The Directive acknowledges in Recital 8 the technological strides emerging through the internet. It notes that these necessitate an "approach which is open to various technologies and services capable of authenticating data electronically." Therefore, although striving to achieve technological neutrality, the Directive is in reality closely linked to the current dominant technology which is based on public key cryptography to produce advanced electronic signatures.

7.144 The prevailing technology underscoring the Directive is that of PKI albeit phrased differently. An example of this is that in the Directive the private key is referred to as "signature creation data" which means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.[72] In turn the decoding public key is referred to as "signature verification data" which means unique data, such as codes or private cryptographic keys, which are used for the purpose of verifying an electronic signature.[73] The Directive outlines in considerable detail a regime for "advanced electronic signatures" created by a "secure-signature-creation device" and supported by "qualified certificates". The result of using this technology is an electronic signature to which member states must give legal effect as they would to a handwritten signature. There are however no presumptions of attribution which is a potential weakness in an otherwise strong technology.

(b) Executing a Signature in Irish Law

7.145 As noted above, there is no strict definition of what constitutes a signature in Irish legislation. Thus while the notion of a traditional signature gives an image of a handwritten mark, written on paper by a signatory, other forms of signing have been endorsed by the courts. These include a typed letter on headed note-paper but which was not personally signed as in *Casey v Intercontinental Bank*.[74] Marks made by rubber stamps and initials have also been deemed sufficient[75]. Therefore manual signatures can cover a wide range of types of embossing including hand-written manual signatures, typewritten

---

72 Directive 1999/93/EC Art 1 (4).

73 Art 2 (7).

74 [1979] IR 364.

75 *Chicester v Hobbs* (1866) 14 LT 433*; and Bennett v Brumfitt* (1867) LT 3 CP 29 *; cf Kelly v Ross & Ross* , High Court, 29 April, 1980.

signatures and stamps so long as it fulfils the functions of identifying the signatory, and evidences his intention to adopt the contents of the document.[76]

(i) The Standards of Electronic Signatures Under Article 5(2) Directive

7.146 The introduction of the Electronic Signatures Directive served to remove uncertainty regarding the legal status of electronic signatures generally and to establish a commonality for the operation of electronic signature services across the European Union.

7.147 The regulatory regime for electronic signatures is outlined in Article 5 (2) of the Directive. An "electronic signature" is defined in the Directive as:

> "[d]ata in electronic form which are attached to or logically associated with other electronic data and which serves as a method of authentication."

7.148 Despite any underlying preferences, the outlook of the Directive aspires to be technologically neutral and the definitions used here are sufficiently broad enough to accommodate "a name or initials typed at the end of an e-mail; a scanned image of a handwritten signature that is attached to an electronic document; and a PIN number used to access a bank account"[77] which would all qualify as electronic signatures under the Directive.

7.149 The legal effects of an electronic signature are discussed in negative terms and the Directive aims at functional parity between electronic and manual signing. Member States are to ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

1. in electronic form; or
2. not based on a qualified certificate ; or
3. not based on a qualified certificate issued by an accredited certification-service-provider or
4. not created by a secure signature-creation device.

7.150 Advanced electronic signatures are addressed in Art.5(1) and are based on a qualified certificate. These are created by secure-signature-creation devices and are calibrated so as to be uniquely linked to and to identify with the signatory, created using means that the signatory can maintain under his

---

[76] McDonagh and White, Electronic signatures: the legal framework and the market reality in Ireland, (2003) 10(8) CLP 228.

[77] *Ibid.*

control. This is also, crucially a signature linked to the data to which it relates so as to make any subsequent change in the data detectable.[78] The directive lays down that such a signature shall be legally equivalent to handwritten signatures in the paper world and are admissible in legal proceedings.

7.151 To reach this level of equivalence with handwritten signatures an advanced electronic signature must first pass over a number of hurdles. The minimum content of a qualified certificate is set out in Annex I of the Directive and must specify that the certificate is issued as a qualified certificate, the identification of the certification service provider and the State in which it is established as well as the name of the signatory.

7.152 Secondly, Annex II sets out the requirements which the certification service providers issuing qualified certificates must satisfy in order to function. The elements and regulation of these Certification Service Providers and Certification Authorities will be discussed further below. For functionality, certification service providers must demonstrate the reliability necessary for providing certification services to ensure the operation of a prompt and secure directory and a secure and immediate revocation service. As a preliminary to certification the Certification Authority must ensure it has sufficient particulars so that the date and time when a certificate is issued or revoked can be determined precisely.

7.153 Thirdly, Annex III deals with the minimum requirements for secure signature-creation devices including the requirement that the signature creation data (the private key) used for signature generation can occur only once, and that their secrecy is reasonably assured. This means that the signature creation data (the private key) used for signature generation cannot, be replicated or discovered. It is also stipulated that the signature be protected against forgery using currently available technology and the signature creation data (the private key) used for signature generation can be readily protected by the legitimate signatory against external intrusion by others.

7.154 The scheme in the Directive is a means to authenticate electronic signatures and through this an attempt to guarantee the authenticity of the electronic or automated documents. This is a mechanism which is implementation-dependent on the Member States through their national legislation.

7.155 What would be the position in the Directive where for example, a handwritten signature had been scanned and was provided by a user to a third party? Could the Directive act to regulate and authenticate such an instrument? This is not an authentication method for the document to which it is attached.

---

78 Art 2(2).

However, it could in theory be retained and used to authenticate other signatures received by the third party in future transactions. This also calls into question the reasons for which electronic documents are signed ie to authenticate the document and also to indicate acceptance of the terms contained therein.[79] It is likely though that the terms of the Directive would be construed broadly given the expressed aim of facilitating the use of electronic signature mechanisms and to bolster their legal effectiveness.

7.156 The Commission invites submissions as to whether it should be provided in the proposed legislative framework that an electronic signature based on a Public Key Infrastructure (PKI) or a similarly tested or testable technology should be required for certain designated transactions.

(2) The US Approach

7.157 As an example of state legislation defining a signature, the *Mississippi Digital Signature Act of 1997*, Section 3 (g) defines "signature" as:

> "any word, group of letters, name including a trade name or assumed name, mark, characters or symbols made manually, by device, by machine or manifested by electronic or similar means, executed or adopted by a party with the intent to authenticate a writing."

7.158 UETA in its turn describes an electronic signature as any:

> "electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record".[80]

7.159 The primary focus of the signature under the US law is to apportion the intent of the party which is inferred by his signature rather than its format.

7.160 This definition includes as an electronic signature the standard webpage click through process. For example, when a person orders goods or services through a vendor's website, the person will be required to provide information as part of a process. When the customer arrives at the last step and clicks "I agree," the person has adopted the process and has done so with the intent to be associated with the record of that process. The actual effect of the electronic signature will be determined from all the surrounding circumstances, however. The adoption of the process may also be viewed as carrying the intent to do a legally significant act, the hallmark of a signature ie conveying the intent of the party to transact.

---

79 *Clipper Maritime Ltd v Shirlstar Container Transport Ltd (The Anemone)* [1987] 1 Lloyd's Rep. 546.

80 UECA (US) section 2(8).

7.161 An important aspect of this definition lies in the necessity that the electronic signature be linked or logically associated with the record. In the paper world, it is assumed that the symbol adopted by a party is attached to or if located somewhere in the same paper that it is intended to authenticate eg, “an allonge” firmly attached to a promissory note, or the classic signature at the end of a long contract. These tangible manifestations do not exist in the electronic environment and accordingly, this definition expressly provides that the symbol must in some way be linked to, or connected with, the electronic record being signed. A digital signature using public key encryption technology would qualify as an electronic signature, as would the mere inclusion of one’s name as a part of an e-mail message - so long as in each case the signer executed or adopted the symbol with the intent to sign.

7.162 Taking the Mississippi model as an example of US law in the area, the legislation adopted and integrated the common law of Mississippi and took a flexible view of signatures. Under the US common law tradition, a signature can be examined as a symbol which has been adopted with no intent to actually sign. Although technologies evolved and the means of conducting commerce shifted, the US judiciary never really moved to exclude electronic signatures as non-valid or legally ineffective signatures. This has been the case since the earliest forms of electronic communication for instance a signature by telegram or a mark or symbol made on a will by a testator.

7.163 In addition the US Government enacted the *Electronic Signatures in Global and National Commerce Act 2000* (E-Sign) which follows the language of UETA by approving a signature as legal where it is made up of any symbol including where this takes electronic form. This includes an electronic symbol adopted with the intent to take responsibility.

7.164 This Act establishes, to the greatest extent possible, the equivalency of electronic signatures and manual signatures. Therefore the term “signature” has been used to connote and convey that equivalency. The purpose is to overcome unwarranted bias against electronic methods of signing and authenticating records. The term “authentication,” used in other laws, often has a narrower meaning and purpose than an electronic signature as used in this (US) Act. However, an authentication under any of those other laws constitutes an electronic signature under this Federal Act.

(3) The Canadian Approach

7.165 The Canadian Law incorporated the language of the UN Model law following the Uniform Law Conference of Canada which adopted the *Uniform Electronic Commerce Act* (UECA) on September 30, 1999, and recommended

its incorporation in all provinces and territories of Canada and the federal government.[81]

7.166 The Canadian definition of an electronic signature includes information in electronic form that a person has "created or adopted in order to sign a document and that is in, attached to or associated with the document."[82]

7.167 Both of these statutory provisions as well as the Model Law on Electronic Commerce can be seen as a species of levelling legislation. They do not attempt to change the substance of the existing law. Their aim is to achieve neutrality of form for and increase confidence in electronic systems and commerce by making the regulatory provisions equally applicable to both paper and electronic documents.

(4) The English Provisions

7.168 In England the relevant implementing legislation is the *Electronic Communications Act 2000*. For the purposes of identifying a signatory through a trusted third party, the UK Government is granted powers to introduce a voluntary accreditation scheme for commercial entities which offer digital signature services.

7.169 The government is also granted powers to amend references to a "writing", "signature" and "paper" in existing legislation to make it clear that these requirements may be met electronically. This is a proactive element in the legislation.

7.170 In England the statutory footing for electronic signatures can be seen in section 7 of the *Electronic Communications Act 2000* which represents a technologically neutral definition of a signature and adopts a broad and purposive approach to regulating these means of electronic documentary verification.

7.171 Prior to the recent European Directive and the implementing national legislative intervention, the identification and verification of electronic documents by electronic signatures was governed by the common law. A prime example is the 2006 English case of *Mehta v J Pereira Fernandes SA.*[83] These proceedings emerged following a petition to wind up a company and an email offering a guarantee to honour a commercial transaction. The appellant instructed his staff to send an email offering a guarantee to the solicitors of the

---

81 Proceedings of the Uniform Law Conference of Canada 380, online at: http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1.

82 UECA (Canada) section 1 (6).

83 [2006] 2 All ER 891.

respondent company (JPF). The email was not signed but bore unmistakeable meta-data in the header which identified the document as having come from "nelmehta@aol.com" which had appeared on all other correspondence between the two including other emails which had also been otherwise signed.

7.172 Mehta later reneged on the undertakings contained in the email and acceptance of which had allegedly been given by the respondent's employees by telephone. Mehta countered that his email address had been typed into the header by an employee without authority. The judge dismissed this in the District Court as untenable. The thrust of the matter then became whether there was no guarantee expressly signed by Mr. Mehta and whether the "electronic signature" could be taken as a true electronic signature so as to verify the document. The District Judge had been of the opinion that the email itself formed the guarantee so as to satisfy the *Statute of Frauds* and that the email address was a signature for the purposes of section 4.

7.173 The High Court debated whether the email qualified as a memorandum so as to satisfy section 4 requirements or whether it was a contractual offer instead.[84] In *Mehta* the offer was a written offer albeit one which was accepted orally.[85] Pelling J in the High Court determined that the email did reach the standards of section 4.

7.174 Turning to the matter of the signature, he conceded that the email was not signed in the "conventional sense" and laid down a useful guide on just how electronic communications should be approached when determining the parties involved. He noted that when discussing emails it was colloquially accepted that the authenticating identifiers are not inserted by the sender "in any active sense. It is inserted automatically." There was no technical or scientific evidence forthcoming in support of Mr. Mehta's contention that his employee had inserted the email address at the head of the communication and the opposition proposed that the email had been signed by the employee as an agent.

7.175 The Court approached the question as strictly one of whether the document was signed at all. The address on the email was compared to the "email equivalent of a fax or telex number." The court relied on *Evans v Hoare* where Cave J had stated that in order to be accepted as a signature the name of the party to be bound must be "intended for a signature" which in the current case it was unlikely to have been.

---

84 As determined in *Evans v Hoare* [1892] 1 QB 593.

85 See *Parker v Clark* [1960] 1 WLR 286.

7.176 The Court then examined the dicta in *Caton v Caton*[86] which stated that a "signature" to be counted as such must be inserted so as to have the effect of "authenticating the instrument". Lord Westbury noted[87] that if the signature occurs only incidentally it cannot have sufficient legal effect so as to authenticate the whole of the memorandum.

7.177 The judge in *Mehta* concluded that "if a party creates and sends an electronically created document then he will be treated as having signed it to the same extent that he would in law be treated as having signed a hard copy of the same document. The fact that the document is created electronically as opposed to as a hard copy can make no difference." Pelling J again drew the issue back to whether an automatically inserted email address after the document had been transmitted would qualify as a signature and concluded that it was in fact ancillary to the contents of the record and divorced from its aim. It was not therefore a signature to satisfy section 4 of the *Statute of Frauds.*

7.178 The Commission turns now to briefly outline the legislative instruments functioning in this jurisdiction before going on to fully outline the technologies involved in executing electronic signatures and how they provide fixity and reliability for the legal admissibility of computer derived documentation.

(5) Ireland

(a) The Use of Electronic Signatures in Ireland

7.179 Electronic signatures are widely used in Ireland in an unregulated and more casual fashion both knowingly and unwittingly. A rudimentary example of this is where a person includes their name at the end of an e-mail message. More sophisticated examples of electronic signatures include secure e-mail, which is offered for example by Post.Trust,[88] eBanking services which are available from banks in the State, of the Revenue Online Service (ROS) which allows for the filing of tax returns online,[89] and Companies Registration Office (CRO) which allows for the electronic filing of annual returns by companies.[90]

7.180 Under the Electronic Signatures Directive as implemented by the *Electronic Commerce Act 2000*, all of these signatures are treated as legally

---

86 (1867) LR 2 HL 127.

87 (1867) LR 2 HL 127 at 143.

88 See www.posttrust.ie.

89 See www.revenue.ie/services/ros/main.html.

90 See www.cro.ie.

equivalent to a traditional handwritten signature and so may be used in evidence to prove the identity of the signatory from which to infer his intention to sign and to adopt the contents of the document.

7.181 The Commission understands that in reality very few of the electronic signatures currently used in Ireland satisfy the requirements of an Art 5(1) signature. The Commission also understands that there is little demand for such thorough Art 5(1) electronic signatures As the situation stands, companies are placed on a European register which classifies them as "in good standing" for the purposes sought. By contrast, while electronic documents in Ireland are "authenticated" they are not "qualified" which from a purely technical perspective represents a different and more thorough layer of security. This will be discussed below along with how well the *Electronic Commerce Act 2000* is suited to and achieves its stated aim.

7.182 The *Electronic Commerce Act 2000* followed an August 1999 discussion paper which the Department of Public Enterprise released entitled "Outline Legislative Proposals on Electronic Signatures, Electronic Contracts, Certification Service Provision and Related Matters". The 2000 Act enabled the State to meet its obligations under the EU Electronic Signatures Directive 1999/93/EC and the Electronic Commerce Directive 2000/31/EC which was an attempt to legislate for the recognition of electronic commerce in its broadest sense including e-government, electronic signatures, electronic contracts, electronic writings and electronic commerce through the promotion of electronic signatures and by providing a legislative basis for accredited certification service providers in the State.[91] The 2000 Act though maintains, however, a distinction as between the differing species of "electronic signatures" and "advanced electronic signatures".

7.183 The difference between the lower grade electronic signature and a digital, advanced electronic signature goes beyond form and in fact provides two key evidentiary elements. The advance electronic signature is capable of providing a higher level of authentication to the signer because, based as it is on PKI, it cannot be easily forged unless the signer loses control of his private key (the binary process for creating such a signature is discussed above).[92] From this perspective the advanced electronic signature would form a sound basis for guaranteeing the integrity for evidential purposes of the content of a digital document. This kind of advanced signature has a strong juridical value in that it warranties the authentication, confidentiality and integrity of the text

---

91 Ryan, "*Legislating for an Electronic Environment: a commentary on the introduction of the Electronic Commerce Act 2000*", [2000] Hibernian Law Journal 256.

92 See paragraph 7.63.

received as being the same as the text sent and that guarantees that no modifications have been made in so far as it is capable of detecting them.[93] It also provides for non-repudiation where the sender cannot say that he did not send the digital document in question and nor can the recipient claim that he did not receive it.

(6) Ireland's Obligations under the E-Sign Directive as addressed through the Electronic Commerce Act 2000

(a) Introduction

7.184 The *Electronic Commerce Act 2000* attempts at one stroke to implement the Electronic Signatures Directive, and the Electronic Commerce Directive. Its evidential utility relates to electronic signatures and in its stated aim of eventual parity (albeit with certain exceptions pertaining to legislation requiring a specific form of signing for eg a will, a codicil, or any other testamentary instrument, a trust or a Power of Attorney), as between advanced electronic signatures and their traditional hard-copy counterparts. Electronic signatures therefore are to have the same legal effect as conventional signatures enforced by the provision that misuse of electronic signatures or any fraud connected with these signatures will be considered offences under the *Electronic Commerce Act 2000*.

7.185 The provisions of the *Electronic Commerce Act 2000*, a technology-neutral statute nevertheless make provision for the activities of persons who certify the identity of signatories of technology-based documents and it sets up a voluntary accreditation scheme for this regulation. It does not however go further and require the mandatory adherence with recognised standards for reliable technology in this area.

(b) Substantive Provisions of the Electronic Commerce Act 2000

7.186 Part 2 of the *Electronic Commerce Act 2000* provides for equivalence as between the electronic and paper documentary worlds as regards writing, signatures, documents under seal, originals, and contracts. The objective of these provisions is to secure equal legal status between manual signatures and electronic signatures in Irish law.

7.187 Section 2(1) of the 2000 Act defines "electronic signature" and "advanced electronic signature" in terms very similar to those used in the Directive. Additionally, "electronic" is defined in the Act to include:

> "electrical, digital, magnetic, optical, electromagnetic, biometric, photonic and any other form of related technology."

---

[93] This is made possible because modifications to the communication can be observed by referencing the hash function and message digest.

7.188 The principles of non-discrimination and legal equivalence and recognition of electronic signatures are provided for in sections 9, 13 and 22 of the *Electronic Commerce Act 2000*. Section 9 contains the fundamental principle upon which the legislation is based which is that information cannot be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form. More particularly, section 13 provides that where the use of a signature is required, an electronic signature may be used provided two conditions are met. These are that:

1. Where the recipient is a public body, any information technology or procedural requirements imposed by that body must be complied with.

2. The person or body to whom the signature is addressed must consent to the use of the electronic signature.

7.189 Section 22 authorises the admissibility of electronic communications and electronic signatures in legal proceedings. Therefore electronic evidence is admissible in legal proceedings and will be afforded the same evidential value as traditional forms of paper evidence. This principle can be seen in the criminal sphere in the *Criminal Evidence Act 1992*, section 5(1)(c).

7.190 The huge importance and evidential scope of section 22 is clear from the standard of definitions which it employs and which are given in section 2 of the Act. The Act is of potential significance in proceedings and tribunals to settle difficulties relating to adducing evidence which may arise in the field of electronic commerce. To this end “legal proceedings” are defined in section 2(1) as “civil or criminal proceedings, and includes proceedings before a court, tribunal, appellate body of competent jurisdiction or any other body or individual charged with determining legal rights or obligations” demonstrating the potentially wide-reaching application of the Act.

7.191 It should further be noted that the distinction and the higher standards imposed on and the securities granted to advanced electronic signatures as against electronic signatures which derive from the Directive are maintained in these provisions. The necessity of achieving functional equivalence runs like a vein through this section and under subsections 9, 13 and 22. All generic “electronic signatures” (electronic signatures simpliciter, advanced electronic signatures, or qualified electronic signatures) are recognised as on a legal par with manually executed signatures. This has a direct impact on their being admissible as evidence in legal proceedings.

(c) The Success of the Electronic Commerce Act in Implementing the Directive: a need for Reform?

7.192 The Electronic Commerce Act reaches, like its counterparts for functional equivalency as between electronic and manual signatures. Functional equivalence acknowledges the differences which exist between manual and electronic signatures and attempts to rank the means of signing equally rather than engaging in a legal fiction by creating an artificial link between the two. Instead the legislation performs a levelling exercise. This regulates electronic signatures so as to enable them to perform the same commercial and evidential functions as written signatures.

7.193 Section 22 is open to severe criticism because it does not include any safeguards in how it applies to the admission of electronic evidence. This is clear when it is remembered that electronic evidence may raise issues relating to reliability given the ease with which such evidence can be fabricated or altered without knowledge or consent.[94] An issue with section 22 though is that it does not detail any requirement of advance notice prior to the use of electronic evidence.[95] This could potentially place the opposing party at a disadvantage where that person is unaware that certain evidence is to be tendered in proceedings in an electronic form and is therefore unable to produce rebutting expert evidence.

7.194 Given the problems of establishing the reliability of electronic documentary evidence, a trial judge would be required to give a caution to the jury where the case rests substantially on the basis of the veracity and reliability of the electronic evidence.[96]

7.195 Under a strict reading of the Directive, it might appear that the Irish provisions do not fully implement Art 5. Yet it must be remembered that under Irish law traditional manually executed signatures do not benefit from any presumptions of validity and are simply assessed on a case-by-case basis in order to determine their legal status.[97]

---

94 See Lambert "*The Search for Elusive Electrons: Getting a Sense for Electronic Evidence*", (2001) 1 (1) JSIJ 23.

95 *Ibid*, at 44-45.

96 See *People (AG) v Casey (No. 2)* [1963] IR 33 at 37-38 on the demonstrated unreliability of certain traditional forms of evidence.

97 Section 10 is an exclusionary provision and extends various exemptions from the principal provisions of the *Electronic Commerce Act 2000* to stated laws. These include those relating to electronic signatures and include wills, trusts and Powers

7.196 A heavier burden is imposed where a signature to a document which requires witnessing or where a seal is required to be fixed to a document. In these circumstances, the legislation requires the use of an advanced electronic signature. For instance, section 14 provides for a signature to be witnessed electronically but contains a number of conditions:

i) the signature to be witnessed must be an advanced electronic signature, based on a qualified certificate, of the person or public body by whom the document is required to be signed;

ii) the document must indicate that the signature of that person or public body is required to be witnessed;

iii) the signature of the person purporting to witness the signature to be witnessed must be an advanced electronic signature, based on a qualified certificate; and

iv) the receiver of the document to be witnessed must consent to the electronic witnessing and any procedural requirements imposed by a public body must be complied with.

7.197 Section11 provides that certain laws are not affected by the provision of the *Electronic Commerce Act 2000*. These are:

(a) any law relating to taxation or other Government imposts;
(b) the *Companies Act 1990 (Uncertificated Securities) Regulations 1996*[98]
(c) the *Criminal Evidence Act 1992*; or
(d) the *Consumer Credit Act 1995*, or any regulations made thereunder and the *European Communities (Unfair Terms in Consumer Contracts) Regulations 1995*.[99]

7.198 McDonagh and White[100] speculate that as technologies progress, these exclusions from the mandate of the legislation will be removed. Crucially it is worth noting that the Act makes it clear that nothing in its provisions can require a person or public body to use an electronic signature and therefore while it promotes an equalised technological environment and means by which

---

of Attorney as well as interests in real property, affidavits, and declarations and the rules, practices and procedures of a court or tribunal.

98 S.I. No. 68 of 1996.

99 S.I. No. 27 of 1995 and S.I.No. 307 of 2000.

100 McDonagh and White, "*Electronic Signatures: the Legal Framework and the Market Reality in Ireland*", (2003) 10(8) Commercial Law Practitioner, p 228.

to verify e-documents, it does not go so far as to force electronic transacting onto parties who are not amenable to participate in electronic transfers etc.[101]

7.199 The Commission provisionally recommends that the distinction between basic electronic and advanced electronic signatures should be retained, and that while the use of advanced electronic signatures should continue to be promoted this should not undermine the use of basic electronic signatures.

(7) Issue of consent in the Electronic Commerce Act 2000

7.200 Parties remain free to prescribe their own terms as to how to verify and conclude electronic transactions and it is this which makes the consent rule absolutely fundamental in a piece of legislation which is presented as being technology-neutral. This consent provision is a feature of many legislative regimes relating to electronic signatures and evidence.

7.201 In Canada for example the consent rule is in UECA section 6 and states that "nothing in this Act requires any person to use or accept information in electronic form…" while in the US section 5 of the UETA applies so that the "Act applies only to transactions between parties each of which has agreed to conduct transactions by electronic means." The UETA provides in subsection 5 (c) that a party who consents to conduct a transaction electronically retains the power to refuse to conduct other transactions by electronic means. Comment 5 to that section notes some limits to this right of refusal. The UECA is silent on the point, but the policy is not likely to be held to differ. This means that the use of electronic signatures and technologies is transaction specific.

7.202 As a result of the consent provision in section 12 (c) *Electronic Commerce Act 2000*, the fact that an electronic signature satisfies the legal requirement for a signature does not make that signature effective against someone who does not want to deal electronically at all. Only the proposed user can make that judgement at his or her discretion. It is also important to note that the consent need not necessarily mean giving blanket consent. One may accept some kinds of information in electronic form and reject others, or accept it for some purposes, or accept electronic documents but not electronic signatures.

7.203 On the other side this may serve to stall transactions rather than facilitating them as the provisions do not envisage rolling consent. Instead it must be sought on a periodic basis (although it is likely that this could be inferred from a previous course of conduct). This may be appropriate and even prudent in the current climate where technological literacy is by no means widespread and it is suggested that in the coming years, as comfort in

---

101 *Electronic Commerce Act 2000*, section 24.

electronic means of transacting and from a legal standpoint discovering and adducing evidence becomes more frequent these safeguards may be relaxed and a more rigid statutory framework implemented.

7.204 The Commission provisionally recommends that the current non-statutory scheme for regulating digital certification service providers be retained but should be reviewed 5 years after the Commission's proposed statutory framework for documentary evidence is introduced.

(8) The Liability of Certification Authorities/ Certification Service Providers under these Legislative Schemes

7.205 The Electronic Signatures Directive establishes a set of minimum requirements with regard to liability that must be implemented by Member States. It leaves it open to Member States to impose additional requirements. The liability provisions operate by imposing liability on Certification Service Providers that issue certificates to the public or that guarantee such certificates to the public. Such Certification Service Providers are liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate.[102]

7.206 While member states are free to derogate as to the level of liability to be imposed, the Directive does instruct that, at a minimum, certification authorities are held liable in damages for loss caused to a party to a transaction who reasonably relies to his detriment on a qualified certificate. The Certification Authority is liable under article 6 for the accuracy of the information contained therein unless the Certification Authority was not negligent in carrying out the certification process. A reverse burden of proof applies in that the Certification Service Provider will be liable unless the Certification Service Provider can prove that it has not acted negligently.[103]

7.207 The Directive seeks to alleviate the burden of liability borne by Certification Service Providers although it requires Member States to ensure that a Certification Service Provider may indicate in a qualified certificate, limitations on the use of that certificate. Such limitations must be recognisable to third parties. Member States are required to ensure that Certification Service Providers may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used. Again the limit must be recognisable to third parties and in such circumstances the Certification Service Provider will not be liable for damage resulting from this maximum limit being exceeded under article 6(4). The Directive is also limited in its extension and

---

102 Section 22.

103 Art 6 (2).

states that the provisions regarding liability shall operate without prejudice to the Directive on unfair terms in consumer contracts.[104]

(9) Types of Certification

(i) Certification Authority Certificates

7.208 This type of certificate certifies the Certification Authorities public key and is used to certify other certificates.

(ii) Server Certificates

7.209 These certificates certify a secure server's public key and must be verified and attested to by a recognised certification authority.

(iii) Personal Certificates

7.210 These certify an individual's public key and indentify that individual to other individuals, to network servers and to other certification authorities.

(10) Trusted Third Parties- Certification Authorities and Certification Service Providers

7.211 When transacting with the key pair it must be remembered that the key pair has no inherited connection with any individual and therefore difficulties as to party identification in blind party transacting remain. The potential weakness in a PKI system is proving who actually participated in a particular transaction. For evidential purposes, how can the chain of custody be guaranteed and linked to a specific individual or entity. How can a person/entity be unconditionally associated with a particular key pair and, consequently establish the integrity of the document for admission as evidence?

7.212 This is not an issue where there is a prior contractual relationship or where the parties transact over a closed network for instance EDI. Electronic data interchange (EDI) is based on electronic interface and a computer-to-computer exchange of business data in standard formats. It requires no human agency as the information is organised according to a pre-specified format that is set by both parties. In such instances the parties are either known to each other or have prior transactive form and can easily and safely communicate the public key of the key pair.

7.213 E-Commerce has now evolved from a local, bilateral level to a multilateral one through the use of the "www" domain on the internet. Symptomatic of the rise of e-commerce has been the progression from face to face transactions to a situation where most transactions occur among strangers

---

[104] Council Directive on unfair terms in consumer contracts, Directive 93/13/EEC, [1993] OJ L95/29.

who usually have no prior contractual relationship and following on from this, the authentication procedure is not a simple task. Where transactions occur outside an EDI context (which is the closest electronic analogy to a face to face transaction) and in the absence of a secure communications channel, the non-repudiation of digital signatures can be guaranteed by the involvement of trusted third parties in the form of certification authorities.

(a) Certification Authorities Explained

7.214 A certification service provider or certification authority is the term granted to a trusted third party in the context of e-commerce. This is the term given to a body which issues electronic signatures to facilitate the transactions of parties with which they have no relationship and in whose communications they play no part. A Certification Service Provider is defined as an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. Other services might include registration services, time-stamping services, directory services and computing services.

7.215 Under the Electronic Signatures Directive if a Certification Service Provider is issuing an advanced electronic signature to the public then it must fulfil certain requirements. These requirements are of a prudential nature and include employing personnel who possess sufficient knowledge and skills and operate with transparency and employ secure and unbiased systems.

7.216 A certification authority undertakes the confirmation of the identity of the subject of an advanced electronic signature and issues a digital certificate which links a public key explicitly to the indentified party. Depending upon the level of inquiry engaged in so as to confirm the identity, the certification service provider provides the recipient of a document with a variable level of confidence as to the authorship of the document and which is reflected in the limitation of the liability they take upon themselves.

7.217 The certificate authorities are currently regulated in Ireland under Part III, section 29 of the *Electronic Commerce Act 2000*. This regulation is in itself loose in that there is no requirement for any certifying authority who wishes to enter the market to obtain the prior authorisation of a central regulating authority before providing certification or other services relating to electronic signatures and issuing certificates under section 29 (1).

(b) Accredited Certification of Certification Authorities in Ireland

7.218 As a means of ensuring acceptance for electronic signatures, end-users must have complete trust in the services of a Certification Authority. Therefore under Article 3 (2) of the Directive, the EC recognised the benefits of an accreditation and certification scheme for Certification Service Providers. In Ireland the basis for a facility for such a scheme is available under the *Electronic Commerce Act 2000*.

7.219 Section 29 of the *Electronic Commerce Act 2000* seeks to implement Art 3 of the Directive. Section 29(1) provides that a person or public body is not required to obtain the prior authority of any other person or public body before establishing itself as an entity providing certification services relating to electronic signatures. The issue of voluntary accreditation is dealt with in section 2(2). This section of the Act empowers the Minister for Communications to introduce a scheme of voluntary accreditation of certification service providers for the purpose of fulfilling the State's obligations under the Electronic Signatures Directive and with an aim to "enhance levels of certification service provision in the State." Under these provisions, the requirements of accreditation authorities were cemented following consultation with the Minister for Enterprise, Trade and Employment. The regulations may designate accreditation authorities and prescribe such matters relating to their designation, as the Minister thinks appropriate which may include setting out:

> "(i) the rights and obligations specific to the provision of certification services of participants in a scheme of voluntary accreditation, and
>
> (ii) the manner in which the accreditation authority designated under paragraph (a) shall elaborate and supervise compliance with those rights and obligations in accordance with the Directive and, in particular, Annex II."

7.220 To be certified under the national accreditation scheme, Certification Service Providers must demonstrate four requirements:

> 1. They must issue qualified certificates in support of advanced electronic signatures which comply with Annex I of the Directive
> 2. As a Certification Service Provider they must be capable of demonstrating compliance with Annex II of the Directive
> 3. They must operate an information security management system in keeping with recognised standards, and
> 4. They must be capable of demonstrating compliance with the Data Protection Directive 95/46/EC.

(11) Supervision and Accreditation in Ireland

7.221 Section 29(5) of the *Electronic Commerce Act 2000* deals with the issue of liability of accreditation authorities. It provides that no civil liability is to be imposed on such bodies in respect of any determination made by them in good faith in the performance of a function under the accreditation scheme.

7.222 While a light regulatory touch is adopted in respect of the entry into the market of Certification Service Providers, the need to protect consumers is recognised by provisions relating to supervision of Certification Service Providers. Article 3(3) of the Directive requires Member States to ensure that an

appropriate system for the supervision of Certification Service Providers is established.

7.223 Dumortier points out that pining down the dividing line between the operation of a supervision scheme and imposing a requirement of prior authorisation may be difficult in practice as "national legislators have to find a way to exercise supervision without setting up a system of mandatory examination prior to the commencement of services."[105]

7.224 Recital 13 explicitly leaves open the possibility of private-sector-based supervision systems being used. The obligation to establish a system of supervision applies only in respect of Certification Service Providers which issue qualified certificates to the public.

7.225 While the Act of 2000 leaves open the possibility of more than one accreditation authority being designated, regulations approved the Irish National Accreditation Board as the competent authority responsible for the development and implementation of a voluntary accreditation scheme for certification service providers.

(i) INAB and NSAI Certification and Accreditation

7.226 The INAB, a division of Forfas established in 1985 is the Irish national body with responsibility for accreditation in accordance with the International Organisation for Standardisation (ISO 17000) series of standards and guides and the harmonised EN 45000 series of European standards. This embraces areas such as environmental management systems, products and personnel, testing laboratories, materials inspection, inspection of the practices of public procurement and the procedures of contracting entities in the water, energy, transport or telecommunications sectors.

7.227 There was a considerable time lag before the INAB was designated as the appropriate national body under this provision which may have been the result of a pragmatic wait-and-see approach in terms of market development. Similar provision is made with regard to liability of bodies designated for the purposes of supervision of Certification Service Providers as have been provided for in respect of accreditation authorities.

---

105 Dumortier, "*The European Directive 1999/93/EC on a Community Framework for Electronic Signatures*", Published in Lodder and Kaspersen, "*E-Directives: Guide to European Union Law on E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society and Data Protection*." Law and Electronic Series, Vol 14 Kluwer Law International, pp 33-65.

(ii) The NSAI's role in certification in Ireland

7.228 NSAI was established under the *National Standards Authority of Ireland Act 1996*, to promote and oversee the highest technical standards within the state and to represent Ireland on international bodies, including the European Committee for Standardization (CEN), the International Organization for Standardization (ISO) and the International Electro-Technical Commission (ETSI).

7.229 One of the duties of the NSAI includes its position as a body charged with providing certification services in this jurisdiction. NSAI provides a Certification Service in accordance with the EN 45000 series of European Standards and global ISO Conformity Assessment Procedures. NSAI has been authorised by the Irish Government as a 'Notified Body' to issue 'CE' marks to providers of goods and services that conform to EU standards. The NSAI also acts as an inspection agent for overseas certification bodies.[106]

7.230 The division of labour between the NSAI and INAB can be seen as follows. The Client Services division provides a range of product and management systems certification schemes in Ireland and Europe. The NSAI is a statutory non-commercial state agency and is accredited by the Irish National Accreditation Board (INAB), the Registrar Accreditation Board in the US (RAB – ANSI NAP), the Standards Council Canada (SCC) and the United Kingdom Accreditation Scheme (UKAS).

7.231 In Ireland, in an effort to retain centralised control over the output of any potential certification provider but with sufficient deference to the free internal market, the certifying authority providing electronic signatures may apply to the accreditation authority designated under paragraph (a) to participate in the voluntary accreditation scheme for independent assessment. However there is no real impetus for certification providers to seek prior approval from the Minister.

7.232 The provisions on liability of Certification Service Providers are contained in section 30 of the *Electronic Commerce Act 2000*. Section 30(1) essentially grafts Art 6(1) of the Directive into domestic legislation verbatim. It provides that Certification Service Providers who provide certification services and who issue qualified certificates will be held liable for any damage caused to a person or public body which reasonably relies on the certificate. The same saving principle applies that the Certification Service Provider will not be liable where it proves that it did not act negligently. Section 30(2) goes on to place a duty on every Certification Service Provider who provides a service of issuing certificates (as a qualified certificate) to the public, to take reasonable steps to

106 NSAI Annual Review 2006.

ensure that specific requirements regarding liability similar to those set out in Art 6(1)(a), (b) and (c) are met. Therefore, it appears that the Irish legislation under section 30(1) appears to go beyond this and lay down further safeguards and that liability under the *Electronic Commerce Act 2000* is broader than under the Directive.

7.233 As well as the *Electronic Commerce Act 2000* it must also be remembered that there is scope under the common law for liability to arise in respect of matters not set out in Art 6(1). Dumortier opines that Certification Service Providers can limit their liability through the use of disclaimers. He suggests that it is possible that a disclaimer stating that the Certification Service Provider's liability is limited could be used to prevent reasonable reliance being established.[107]

7.234 The *Electronic Commerce Act 2000* goes beyond the requirements of the Directive and lays down procedures for any eventualities involving revoked certificates and the liability surrounding these is explained in section 30(3). The Directive imposes liability in respect of revoked certificates on Certification Service Providers who issue them while section 30(3) also imposes liability on Certification Service Providers with regard to certificates they have merely guaranteed.

7.235 McDonagh and White question whether it is practical to hold a Certification Service Provider liable for failure to register revocation of a certificate where the Certification Service Provider has merely guaranteed the certificate rather than having issued it.[108] The guaranteeing Certification Service Provider may not itself know that the certificate has been revoked. Liability is two-fold in this instance and imposed not only in respect of failure to register the revocation of the certificate under the Directive but also for failure to publish notice of the revocation or suspension of the certificate "as prescribed".

7.236 Section 30(4) deals with limitation of liability of Certification Authorities. The accreditation/certification scheme ensures Certification Authorities have a mechanism of demonstrating the required levels of independent testing. However this is a market driven exercise and is

---

107 Dumortier, "*The European Directive 1999/93/EC on a Community Framework for Electronic Signatures*", Published in Lodder and Kaspersen, "*E-Directives: Guide to European Union Law on E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society and Data Protection*." Law and Electronic Series, Vol 14 Kluwer Law International, pp 33-65.

108 McDonagh and White, "*Electronic Signatures: the Legal Framework and the Market Reality in Ireland*", (2003) 10(8) Commercial Law Practitioner, p 228.

independently undertaken on an ad hoc basis by those individuals and entities who have most to gain from marketing themselves. Under the Directive an accredited body which demonstrates that it meets the requirements of the Directive and can therefore be taken to be issuing recognised advanced electronic signatures can quite legitimately abrogate any liability which may arise from a loss suffered by a third party depending on this certification.

7.237 Furthermore, in order to ensure the authenticity of the identity and the context of the certificate, the Certification Authority digitally signs it. As it is essential for both parties who use different Certification Authorities to trust each other's authority, there are some methods of certifying the Certification Authority's identity and the authenticity of the issued certificate; self-certification, cross-certification and by establishing a root Certification Authority such as a government agency at the apex of the hierarchy.

7.238 Apart from the civil liability of Certification Authorities, the *Electronic Commerce Act 2000* introduces a number of offences for the fraudulent and unauthorised use of electronic signatures, signature creation devices and electronic certificates. The offences are designed to address any forgery of electronic signatures, and the unauthorised use of electronic signatures. Other offences prohibit the unauthorised use of a certificate for fraudulent or other unlawful purposes and prohibit persons from misrepresenting their identity or authorisation in accepting or requesting certificates.[109]

(12) Need for Further Regulation or Updated Standards?

(a) Summary of Current Legislative Regimes

7.239 The legislative approach to electronic signatures in the United States and Canada is minimalist and technology neutral. This approach shifts responsibility on to the parties to a signature, particularly on the relying party, to decide what kind of electronic signatures they will accept for their transaction. The risk of loss from a fraudulent signature remains on the relying party, as it is for signatures on paper. The major exception to this approach is essentially public sector electronic signatures. Many levels of government are developing digital signature systems supported by certificates to be used in dealings between citizens and the government.

7.240 Other jurisdictions are contemplating whether to legislate to support the reliability of their public key infrastructures, or to set out the duties and liabilities of the parties to certified electronic signatures. The UNCITRAL Model Law on Electronic Signatures and the EU Directive contribute to that process of reflection.

---

[109] Sections 6, 7 and 8 on offences generally and section 25 on the fraud or misuse of electronic signatures and signature creation devices.

(13) Overcoming Evidential Problems

7.241 While advanced electronic signatures are a thorough means of proving that the signed document emanates from a particular identifiable signature, it does not and in effect cannot prove that the now authenticated sender actually transmitted the documentary communication. Verifying electronic documentary evidence is also dependent upon many factors including the number of those with access to a given computer, the security measures taken and the availability of the computer for inspection by the party against whom the evidence is being tendered. For this reason, expert evidence may be called to resolve these problems and robust discovery provisions are necessary to make up for the inherent untestability of the unregulated signature whereas the opposite is the case associated with physical signatures.

7.242 The provisions of the *Electronic Commerce Act 2000* mean that while evidence will still have to meet the thresholds of admissibility faced by all documentary evidence, its evidential value under section 22 can no longer be called into question by virtue of its electronic form.

(14) Summary on Utility of Electronic Signatures and Regulating E-Signatures and Possibilities for Reform

7.243 From an evidential perspective these initiatives aim at ensuring that electronic signatures simpliciter can fulfil the requirements of identification, authentication and non-repudiation by the most reliable means in e-transactions. Their impact however is severely compromised given that they are solely focused on either the electronic signature technology as a technical baseline established by means of a legal instrument, or on legislation, which regulates digital signatures in order to equate them legally to hand-written ones, or on the structure of Certification Authorities and the use of qualified certificates in connection with electronic signature applications.

7.244 This chapter has attempted to define the meanings and perimeters of the varying international models towards e-authentication. To ensure admissible documentary evidence can be extracted from such transactions and communications for litigation purposes and these policies highlight the significance of e-signatures as a means of promoting authenticity and injecting integrity into what is otherwise seen as a temperamental means of conducting transactions electronically.

7.245 The current *Electronic Commerce Act 2000* which implements the spirit of the EC Electronic Signatures Directive operates a system of self-regulation and voluntary accreditation. Whether this is a thorough means of promoting consistency and evidential certainty remains to be seen in that at present the uptake of advanced qualified signatures remains relatively low.

7.246 Wilson has described electronic data as "somewhat amorphous" but it is submitted that with a proper and thorough record management system alien parties will not readily gain access to another's files.[110] While it has previously been argued that any regulation must not foist any undue financial burden onto commercial or private entities in the form of an obligation to proactively show the integrity and reliability of their electronic document generation or transmission machinery, it is proposed that far from recommending a central government hub charged with approving e-signatures and certificate service providers which would fall foul of the competition authority, instead a central agency could, in the future, require those seeking certificates or the certification authorities themselves to demonstrate that they have achieved certain minimum standards and investigated the provenance of the parties they are being asked to attest as valid. This would encourage uniformity and remove the market-orientated bent of those who grant certificates. This minimum regulation would promote true functional equivalency as between digital and hand-written signatures by promoting and growing the number of users which is a means of promoting knowledge of and access to these technologies with minimal interference in the market. This would be achieved through a central government licensing scheme and would reduce the potential for fraud and the potential for repudiation of contracts.

7.247 Arguments against such a scheme would focus on the nature of e-authenticating technologies which are constantly developing and are therefore not as yet capable of being conclusively defined. In such a climate it might then be unwise to attempt regulation on the basis of digital signatures or to set criteria, which only consider certain forms of e-signatures, while leaving space for new technologies to emerge.

7.248 Perhaps the solution would be a move to a more harmonised regime of consumer protection legislation in the area of regulating electronic commerce for evidential purposes. Rather than focusing energy on the task of defining the validity or otherwise of an electronic signature as a means of authentication, should resources be funnelled elsewhere?

7.249 In recognition of this the Commission has provisionally recommended that the current non-statutory scheme for regulating digital certification service providers be retained but that there should be room for review following a period of 5 years after the Commission's proposed statutory framework for documentary evidence is introduced.

---

110 Wilson, "*MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*," Oregon Law Review, Vol 86 No. 4, p 1201-1240.

(15) A Summary of the Achievements of the Electronic Signatures Directive

7.250 The Electronic Signatures Directive represented an exercise in defining the notion of an electronic document and essentially attempted to bring digital and computational witnessing of documents on a functionally equivalent par with the traditional rules of evidence adapting and analogising these traditional black-letter rules to suit the problematic electronic media at hand. Irish legislation in the form of the *Electronic Commerce Act 2000* followed on foot of the Electronic Signatures Directive which was to eliminate any legal differences amongst EU member states when it came to cyber-consumerism.

7.251 The *Electronic Commerce Act 2000* represents a starting point for the promotion and implementation of e-signatures at a domestic level rather than a potential backbone of the European aspect of e-authentication. In fact, the prospect of constant adjustment and recalibration of the provisions of the Directive, to the needs of e-commerce was proved in the meeting of the European Forum on E-business.[111] This compared the different timescales, interpretations and implications of the Directive, with a view to making an electronic signature a more solid and reliable tool and a universal technical and legal standard for adoption.

(16) The Potential for Fraud and Non-Repudiation

7.252 What measures can be taken to ensure against fraud and abuse where electronic signatures are used?

7.253 Just as a notary verifies the intent of the signatory, electronic signatures can use verification methods to insure the signatory understood the purpose and the intent of the signature process.

7.254 The dominant law at play in Ireland concerning electronic signatures as a means of providing stability, market confidence and securing for evidential purposes digital documentary instruments is the *Electronic Commerce Act 2000*. This system attempts to support the use of advanced qualified signatures in the state and pre-empt inconsistent state law at a European level to ensure a harmonised system within the EU. The law as applicable in this jurisdiction is devised so that commercial entities and government agencies should have confidence in using electronic signatures.

7.255 While certified electronic signatures are not necessarily a final incorruptible means of establishing identity authentication, they are more secure than the earlier techniques of password and or physical tokens.

---

111 Available at www.eema.org.

7.256 Electronic signatures are a valuable source of probative evidence towards determining the providence of a document in court where the private key in question has been randomly generated, kept securely and there is nothing to suggest that it has been compromised. Garfinkel and Spafford have suggested that electronic signatures are a "substantially more secure way of having people identify themselves on the Internet than the alternative: usernames and passwords."[112]

7.257 Given that technologies are still developing, and judicial decisions on electronic signatures are relatively few, should the Irish legislature attempt to customise some portions of its application of the directive or leave the continuing development of this area to standardisation bodies producing industry standards in line with ISO and EN MLA harmonisation systems and in tune with the needs of the market?

(17) Concluding remarks on the Area and the Benefits of Electronic Signatures?

7.258 The utility of electronic signatures extends beyond purely commercial entities in e-commerce. It must also be remembered that when an e-commercial transaction is electronically signed, the formal legal requirements (writing, integrity and the originality of signature and document) are satisfied, since the Electronic Signatures Directive places the digital signatures on a par for functional equivalency with its physical counterparts.

7.259 An advanced electronic signature can also be used to irrefutably sign a document. Should an electronic notary receive the signatures of two or more parties a formal record can be made of the agreement between the parties. Using a reliable and verifiable independent time clock to time stamp the receipt of the digital signatures means that the exact time of the commercial transaction can be recorded.

7.260 E-signatures can offer greater reliability and transparency in the field of e-commerce by minimising the risk of unintentionally dealing with frauds or those who may intercept e-communications. They act as a safeguard in detecting message tampering and where they are implemented they mitigate the possibility that digitally represented information has been altered after it was sent.

7.261 The problem of electronic signing is essentially that there are two linked issues to consider. These are the legal approach and associated problems and the strictly technical approach as regards the technological and computer innovations surrounding the signatures. In this latter category the

---

[112] Garfinkel and Spafford, *Web Security and Commerce,* 1997, O'Reilly and Associates Inc, Cambridge, USA, p 133.

signature is, in accordance with technical expertise and standards either valid or not and the prospect of a judge evaluating the validity of the signature is unpalatable to many technical experts.

7.262 The Commission believe that when sufficient comfort levels have been established in fields where e-signatures are of potential use ie commerce and law etc, the uptake of these signatures will grow and provide legal and commercial certainty and add greater strength to the reliability and the security of e-transactions. This would involve strengthening consumer rights in case of fraud, abuse and even human error while keeping the alternative of conventional transactions available to reluctant e-signatures users.

7.263 The EU Directive and the *Electronic Commerce Act* attempt to set out a functional and well-defined legal environment for e-transactions. E-signatures as a technology are in their infancy and many aspects need to be worked out in conjunction with the users and the market's needs. However e-signatures do play a role in authenticating digital transactions and thereby in promoting e-commerce by providing safety and reliability in e-transactions. It is due to the significance of this emerging technology that legislative initiatives struggle to find the best regulatory scheme in order to legally equate e-signatures to the handwritten ones.

7.264 A flexible approach to reforming the law in the area of regulating electronic verification devices is preferable given that there is no real urgency to change the law as it currently applies to electronic signatures.

7.265 At present there is no immediate need to establish a specific State agency to act as a hub with responsibility for the issuing minimum standards or licences to potential Certification Authorities. The Commission encourage the production of Government produced guidelines supported by industry minimum standards on the benefits of conformance with procedural measures to establish the reliability of evidence. This would not interfere with the operation of the free market and instead would operate to monitor the needs and application of the electronic signature law, promote the use of electronic signatures among governmental, private and commercial entities and monitor and make any recommendations for future changes in the law.

7.266 It appears from academic comment as well as executive commentary that it is necessary to provide solid and workable legislation to the area of e-commerce and e-signatures to eliminate incorrect perceptions in the legal environment. Further justification for this can be observed by examining the debate accompanying the second reading of the UK Electronic Communications Bill where it was stated that;

> “Lawyers argue about whether electronic signatures would be recognised as valid by the courts, but we cannot afford to wait while

> lawyers argue and the courts decide. Instead, clause 7 will allow businesses and consumers to have confidence in electronic signatures, because it puts beyond doubt that a court can admit evidence of an electronic signature and a certificate in support of that signature not only to establish from whom the communication came, but to establish the date and time at which it was sent and whether it was intended to have legal effect".[113]

7.267 The Commission does not find it necessary to recommend the introduction of legislation aimed at promoting electronic commerce by providing a special legal infrastructure for certain technologies based on promoting "digital" as opposed to the more generic "electronic" signatures. This could be outlined on the basis of a digital signature which has been verified by a licensed certification authority which may be used to sign a document and have legal force and effect equal to that of a written signature.

7.268 In light of the commentary which proceeded the drafting of the US Uniform Electronic Commerce Act where the Chair stated;

> "Legal uncertainty about the enforceability and admissibility of electronic communications and records is inefficient, creates barriers to electronic commerce, and imposes unnecessary costs of participants in legitimate electronic commerce".[114]

7.269 The Commission is of the view that the absence of litigation in this area is not necessarily symptomatic of a smoothly run system. There is an absence of a general code of practice applicable to certification authorities. Nor is there a means by which to regulate compliance. The current means of voluntary self-regulation fails to allocate adequately the balance of power and associated burdens and liabilities between the providers of certification and those who rely on the signatures in a coherent and meaningful way.

7.270 The Commission does not call for the replacement of the voluntary self-accreditation scheme with provision for regulating certification service providers with a more intrusive legislative regime. While such a legislative scheme would set down mandatory standards, it is felt that in deference to the free market industry minimum standards could operate within the State rather than implementing a governmental licensing scheme. It is submitted that such a supervisory system would be difficult to effectively police. It would be difficult to

---

113 Patricia Hewitt, Minister for Small Business and E-Commerce, HC Deb 29 November 1999 cc 45-6. Available at www.parliament.uk.

114 Professor Patricia Blumfeld Fry, "*Impressions on California's Changes to the Uniform Electronic Transactions Act*", Electronic Commerce and Law Report, December 22, 1999.

distil industry practices to reduce them to a formula and to isolate and extract a workable set of standards for qualified service providers. At present there is no interoperability across Europe and a published "Trusted List" forms the apex of agreement on minimum standards though this is in no way comprehensive.

7.271 Some jurisdictions have attempted a prescriptive rather than a facilitative means of legislating for the area of electronic commerce. Singapore is one such jurisdiction. The *Electronic Transactions Act 2002* sets out to "facilitate electronic communications by means of reliable electronic records."[115]

7.272 A note of caution must underpin any attempt to legislate in the area of electronic signatures as verification tools for electronic documents for evidential purposes. The introduction of legislation to merely facilitate electronic transacting and introduce certainty into the area could be seen as a step too far and represent a layer of legal prescription and bureaucracy where none is needed.

7.273 The danger when attempting to legislate in the manner which the Singapore Executive has undertaken was expressed by the Australian Electronic Commerce Expert Group in its 1998 Report to the Attorney General.[116] The danger identified here was one in which, when dealing with new and emerging technologies the temptation is ever present to:

> "set the standards required of a new technology higher than those which currently apply to paper and to overlook the weaknesses that we know to inhere in the familiar."

7.274 The Commission does not propose to recommend the enactment of legislation in this area at present given the possibility that even imposing minimum standards at a statutory level could lead to injustices by establishing a benchmark for evidential purposes to apply to commercial transactions where there are no equivalent markers applying to paper or oral transactions.

7.275 Instead, guidelines and the development of minimum standards would improve the area without being unduly burdensome and would have the effect of ensuring standardisation of form with knock on legal affects. The Commission thus feels that such non-statutory guidelines should be developed by an expert group comprising relevant State and industry representatives in connection with electronic verification systems, which would encourage the identification and implementation of minimum standards.

7.276 *The Commission provisionally recommends that non-statutory guidelines be developed by an expert group comprising relevant State and*

---

115 Section 3 (a).

116 *Electronic Commerce: Building the Legal Framework*, March 31 1998.

industry representatives in connection with electronic verification systems, which would encourage the identification and implementation of minimum standards.

CHAPTER 8 SUMMARY OF PROVISIONAL RECOMMENDATIONS

8.01 The Commission's provisional recommendations in this Consultation Paper may be summarised as follows.

8.02 The Commission provisionally recommends that the long-established definition in the law of evidence of "documentary evidence" as being a thing in legible form that is capable of being adduced in evidence should be placed within a statutory framework and supplemented by the addition of references to electronic and automated documents and records. [Paragraph 1.32]

8.03 The Commission provisionally recommends that "document" should be defined for the purposes of the law of evidence as "anything in which information of any description is recorded". The Commission also provisionally recommends that this definition of "document" is to be understood as combining electronic, automated as well as hard copy traditional documents and that this definition would apply to both civil and criminal proceedings. [Paragraph 1.33]

8.04 The Commission provisionally recommends that the law of evidence as it applies to documentary evidence should adopt a technologically-neutral approach, in which the essential rules of admissibility should apply equally to traditional forms of manually created documents and to electronic and automated documents and records. [Paragraph 1.36]

8.05 The Commission provisionally recommends that a "public document" should be defined as "a document retained in a depository or register relating to a matter of public interest whether of concern to sectional interests or to the community as a whole, compiled under a public duty and which is amenable to public inspection." [Paragraph 1.41 and 3.28]

8.06 The Commission provisionally recommends the abolition of the Best Evidence Rule, namely the rule of evidence to the effect that an original piece of evidence, particularly a document, is superior to a copy and that if the original is available, a copy will not be allowed as evidence in civil or criminal proceedings. [Paragraph 2.152]

8.07 The Commission also provisionally recommends that, in its place, the proposed statutory framework on documentary evidence should contain a rule that documentary evidence is, in general, admissible in civil and criminal

proceedings where the court is satisfied as to its relevance and necessity. [Paragraph 2.153]

8.08 The Commission provisionally recommends that the rules of evidence concerning the need to produce an original of an electronic or automated document be interpreted to mean presenting a reproduction in legible form (including a printout) or a copy or derivative of an electronic document. [Paragraph 2.213]

8.09 The Commission provisionally recommends that, in general (and as an exception to the exclusionary rule for hearsay evidence), a public document, defined in the manner already provisionally recommended by the Commission, should be presumed to be admissible as proof of its contents, subject to any contrary evidence as to its authenticity. [Paragraph 3.82]

8.10 The Commission provisionally recommends that the well-established distinction between private and public documents, in which there is no presumption of due execution of private documents, should be maintained and that this should be placed on a statutory footing. [Paragraph 3.94]

8.11 The Commission provisionally recommends that the proposed legislative framework on the admission of documentary evidence should provide that "business records" should be presumed to be admissible in evidence, that the term should include those business records referred to in the *Criminal Evidence Act 1992*, namely records kept by "any trade, profession or other occupation carried on, for reward or otherwise" and that the term should also encompass records kept by a "charitable organisation" as defined in the Charities Act 2009. [Paragraph 4.09]

8.12 The Commission provisionally recommends that business documents be accepted as admissible evidence if the document was created or received in the course of a business and where:

a. The information in the statement is derived from a person who had, or may reasonably be supposed to have had, direct personal knowledge of that information;

b. That the documentary statement has been produced for the purposes of a business; and

c. That the information is contained in a document kept by a business. [Paragraph 4.15]

8.13 The Commission provisionally recommends that statements produced in anticipation of litigation ought to remain inadmissible as evidence of matters which they contain, except in certain stated exceptions, such as those involving money laundering as already provided for in the *Criminal Justice Act 1994*. [Paragraph 4.26]

8.14 The Commission provisionally recommends that the court should retain the discretion to refuse to admit business records. [Paragraph 4.161]

8.15 The Commission provisionally recommends the retention of the *Bankers' Books Evidence Act 1879* (as amended), which should be updated to apply to all credit institutions. [Paragraph 4.162]

8.16 The Commission provisionally recommends the adoption of an inclusionary approach to the admissibility of both manual and electronic documentary evidence, subject to a number of safeguards and the continuance of the discretion of the court to exclude the evidence. [Paragraph 5.19]

8.17 The Commission provisionally recommends that electronic and automated documentary evidence be admissible by means of secondary evidence where this is shown to have sufficient integrity, including by reference to the electronic record system used. [Paragraph 5.120]

8.18 The Commission invites submissions as to whether the proposed rule concerning the admissibility of documentary evidence should apply to information supplied by a person who would not be compellable to give evidence at the instance of the party wishing to give the information in evidence. [Paragraph 5.157]

8.19 The Commission provisionally recommends that notarised documents should be admissible in civil proceedings on conditions comparable to those in section 30 of the Criminal Evidence Act 1992. [Paragraph 5.243]

8.20 The Commission provisionally recommends that, in the case of mechanically recorded electronic documentary evidence, if it is shown to be an authentic recording, any defects in the quality of such a recording or a dispute as to the identity of the speaker on the recording will not be a ground for ruling it inadmissible in evidence. The Commission also provisionally recommends that any such issues should go to the weight of the evidence rather than to admissibility. [Paragraph 6.31]

8.21 The Commission provisionally recommends that in light of the Commission's view that the law should be technologically-neutral, no special evidential regime should be introduced to govern the admissibility of computer-generated documents. [Paragraph 6.183]

8.22 The Commission invites submissions as to whether in connection with electronic and automated documentary evidence a distinction should be made as between an "original" and a derivative in admitting documentary evidence. [Paragraph 6.184]

8.23 The Commission provisionally recommends that, in general, a "signature" should be defined as "a writing, or otherwise affixing, of a person's name, or a mark to represent his name, by himself or herself, or by his or her

authority with the intention of authenticating a document as being that of, or as binding on, the person whose name or mark is so written or affixed." [Paragraph 7.24]

8.24 The Commission provisionally recommends that a single term "signature" should be used to describe both manual signatures and electronic signatures but that for the purposes of verification, different definitions should be used for both. [Paragraph 7.124]

8.25 The Commission provisionally recommends that standards for electronic signatures should be developed uniformly, transparently and objectively and that the proposed legislative framework should give specific recognition to electronic signatures that comply with any relevant international standards. [Paragraph 7.134]

8.26 The Commission invites submissions as to whether it should be provided in the proposed legislative framework that an electronic signature based on a Public Key Infrastructure (PKI) or a similarly tested or testable technology should be required for certain designated transactions. [Paragraph 7.156]

8.27 The Commission provisionally recommends that the distinction between basic electronic and advanced electronic signatures should be retained, and that while the use of advanced electronic signatures should continue to be promoted this should not undermine the use of basic electronic signatures. [Paragraph 7.199]

8.28 The Commission provisionally recommends that the current non-statutory scheme for regulating digital certification service providers be retained but should be reviewed 5 years after the Commission's proposed statutory framework for documentary evidence is introduced. [Paragraph 7.204]

8.29 The Commission provisionally recommends that non-statutory guidelines be developed by an expert group comprising relevant State and industry representatives in connection with electronic verification systems, which would encourage the identification and implementation of minimum standards. [Paragraph 7.276]