Professor
Peter Sommer

Peter Sommer combines academic and public policy work with commercial cyber security consultancy, with a strong bias towards legal issues. He has acted as an expert in many important criminal and civil court proceedings where digital evidence has been an issue.

He is currently Professor of Digital Forensics at Birmingham City University and also a Visiting Professor at De Montfort University Cyber Security Centre. Until 2011 he was a Visiting Professor in the Information Systems Integrity Group in the Department of Management at the London School of Economics and a former Visiting Reader, Faculty of Mathematics, Computing and Technology, Open University. As a consultant he is a well established expert on computer security advising stock exchanges, large companies and insurance companies on systems risk.

He is a Fellow of the British Computer Society and also a Fellow of the Royal Society of Arts.

Digital Evidence / Expert Witness Work

Legal expert witness activity has included:

- **R v Michael John Smith** - described by the Security Commission as the UK's most important official secrets case involving scientific and technical espionage
- **Rome Labs / Datastream Cowboy hack**. A major global hacking case with USAF and NASA among the targets initially thought to have been perpetrated from North Korea and Latvia but which turned out to have been by two UK schoolboys. There were hearings in the US Senate at the beginning of the "Information Warfare/Electronic Pearl Harbour" scares. The UK case involved many novel issues of the handling of technical evidence, admissibility and the problems of evidence from US covert agencies

- **R v Alibhai and others.** A large conspiracy involving the commissioning and distribution of counterfeit Microsoft software and money laundering
- **"NCS Operation Cathedral"** - the first large UK Internet paedophile ring. At the end of the trial penalties for the related offences were increased and POLIT, the precursor to CEOP, was set up. At a technical level there were significant issues of case management arising from the large numbers of computers that had to be examined.
- **"DrinkorDie"** - an international investigation into organised software piracy - "warez" groups - led to the charging of 6 UK individuals. Because of the large numbers of computers involved and the extent of complex evidence from overseas agencies - this was a further challenge in terms of case management was well as of basic investigation of the contents of computers. The UK case was one of the most expensive trials in recent years. Also known as National Crime Squad Operation Blossom
- **R v Ying Guo** - illegal immigration conspiracy in which 58 dead Chinese were found in the back of a lorry at Dover. Defendant was a translator on whose computer was discovered apparent draft immigration applications
- **"Chohan family"** - a family killed by a criminal in order to take over a transportation company which was then to be used for narcotic trafficking. Some bodies were never found - a computer was found which held drafts of important documents
- **Godfrey v Demon** - an important Internet defamation case which helped define the extent of the "innocent dissemination" defence available to ISPs
- **R v Waddon** - an obscene publications act case which defines "place of publication" for jurisdictional purpose
- **R v Atkins** - a Protection of Children Act case which clarifies the strict liability test in "possession" and also the nature of the "legitimate research" defence
- **R v Lennon, R v Cuthbert** - two Computer Misuse cases in which the ambit of the 1990 Computer Misuse Act has been clarified
- **Sorrell v FullSix and others** - An aggressively-fought defamation action by the head of the advertising group WPP against Italian former colleagues suspected of publishing defamatory blogs. But the authors had used anonymising facilities to conceal their activities. The case tested the limits of the disclosure rules in relation to forensic artefacts as well as significant technical challenges.
- **The "Red Mercury" terrorist case** - this was an allegation by the News of the World's "fake sheik" that material for a dirty bomb was being offered in the UK. ("red mercury" is a myth and the case was thrown out)
- **Operation Crevice** - the fertiliser bomb terrorist case - 14 months at the Old Bailey.
- **"Scallywag"** - a case under the Representation of the People Act, with place of publication and proof of involvement as the issues. Scallywag was a magazine that claimed to publish stories Private Eye thought too difficult.

- **R v Deamer and others** - large scale narcotics importation from Spain
- **R v Murphy and others** - long-running series of trials involving narcotics importation from Colombia - one issue was the provenance and reliability of overseas intercept material (which is admissible though the UK equivalent s not)
- **R v B and others** - the UK's first "phishing" case involving allegations of money laundering against a number of individuals from a variety of East European countries. The trial against one alleged principal was abandoned as a result of her ill-health
- **R v O** - terrorism. Allegations involving assistance given to Jemaah Islamiah.Charges dropped after defence analysis and submissions
- **Republic of South Africa v Jacob Zuma and Thint** Allegations of corruption against a South African politician, now President of the Republic and the South African branch of a French armaments company. Case eventually dismissed. Large numbers of computers had been seized from Zuma, his alleged associates and from Thint.
- **DPP v Kinsella** Irish narcotics importation case relying on ETSI standard Dutch phone intercepts
- **Pharm-a-Care Laboratories Pty Ltd v Commonwealth of Australia** Large Australian case involving compensation after regulatory action: examination and reconstruction of computers
- **R v Parker & Champkins-Howard** Faked “Banksy” prints and faked email evidence
- **UEA-CRU Independent Climate Change E-mails Review** Support for the Muir-Russell team
- **Inspire v Taylor Drew Productions** Examination of computers to establish that intellectual property relating to computer-generated children’s cartoons had been fully removed.
- **Operation Alpine** Forensic aspect of Major Crime Review of a Lincs Police/CEOP investigation into commercial distribution of IIOC via newsgroup feeds
- **SRA v Gore & Miller** Solicitors’ disciplinary proceedings: letters sent to file-sharers
- **R v Naqshbandi** Cash for Crash insurance fraud
- **R v Preko** Money laundering; charged with James Onanefe Ibori
- **Special Tribunal on the Lebanon / Office of the Prosecutor** Hague-based trial around the murder of Rafiq Hariri
- **International Criminal Court** Case of Uhuru Kenyatta
- **FCA v Steve Graham** Second (and aborted) trial of ISoft director
- **SIAC: Re: Y** Report for Special Immigration Appeals Commission about varying the Internet-access aspects of bail conditions

- **R v Moazzem Begg** Terrorism trial was abandoned after MI5 disclosure but prior to that technical issues about the files that were the subject of charges
- **R v Seth Nolan-McDonough** Newton hearing on extent of damage caused by juvenile accused of "slowing down the Internet" via DDoS attacks
- **R v Tailor & others** "card-sharing" fraud against Virgin cable services
- **Privacy International & others v GCHQ & SoS FCO** Hearing before the Investigative Powers Tribunal on "computer network exploitation" and "equipment interference" powers (on going)
- **"MM" v Home Secretary** Proceedings before the Immigration Tribunal examining alleged fraudulent English language skills testing.
- **AY v Facebook & others** Civil proceedings about speed of takedown in revenge porn claims
- **R v Belton, Mulligan & Gother:** "Interception on public or private network" / RIPA interpretation issues in alleged conspiracy to pervert the court of justice. Analysis of police use of Blackberry Exchange facilities.
- **R v Daniel Kaye:** Large-scale computer misuse. Botnets using IoT devices – the Mirai botnet used against a national cellphone system and with collateral damage in Germany. Alleged attempted extortion of UK clearing banks
- **Encrypted phones in "county lines" narcotics trafficking:** more than 15 instructions for the National Crime Agency and regional Serious Organized Crime Units
- **R v Finch** Official Secrets
- **Operation Venetic** (ongoing): results of the breach of the EncroChat encrypted phone network: instructed by several defence teams to cover evidential reliability and admissibility issues

Other cases have included fraud on a National Lottery terminal, fraud via cloned credit cards, telecommunications fraud via cloned cellular phones, fraud on the Post Office's internal Horizon system, an alleged theft of a large quantity of credit card numbers from hacked e-commerce sites - the credit card numbers were subsequently published as a "boast", allegations of stolen data and computer programs, pirated computer games, and industrial espionage. Civil instructions, not proceeding to litigation, have included requests to define the role of Wireless ISPs and the impact of the use of Internet "scraping" software on the Computer Misuse Act, Regulation of Investigatory Powers Act and the Data Protection Act. Advice has also been provided on the techno-legal aspects of implementing particular forms of behavioral advertising via ISP activity. There have also been a number of "internet paedophile" cases including some under Operation Ore (plus some instructions from the Ministry of Skills and Education about fitness to work with children).

The practical legal work has always gone hand-in-hand with an interest in professionalising digital forensics and developing "the reliability of digital evidence" as an academic discipline both on its own and as part of the broader

Information Assurance agenda. Peter Sommer spoke at some of earliest law enforcement conferences on the subject and continues to do so, including a number of closed conferences. In 1999 he was invited to speak at a FBI conference on cybercrime and in October 2000 he was part of the UK delegation to the G8 Government-Industry Dialogue on Security and Confidence in Cyberspace Workshops in Berlin. In January 2002 he was appointed by the Royal Military College of Science (Cranfield University) as an external examiner to their MSc course in Forensic Computing having previously acted as the external academic evaluator. In April 2002 he became an advisor to the UK's National High Tech Crime Training Centre During 2005 and 2006 he served on a Technical Working Group to develop a training scheme for digital evidence run by the US National Institute of Justice (part of the Department of Justice), one of only two non-US citizens to do so.
In November 2005 the Home Office-backed Council for the Registration of Forensic Practitioners (www.crfp.org.uk) launched a section devoted to digital evidence and Professor Sommer was Joint Lead Assessor from then until 2009. Until recently he also advised the Forensic Science Regulator.

In 2013 he was included in the List of Experts before the International Criminal Court at the Hague.

In 2013 also he was invited by the International Information Systems Security Certification Consortium - $(ISC)^2$ - to act as the only non US reviewer of its Certified Cyber Forensics Professional – CCFP – program.

In 2014 he was appointed to the Home Office Digital Signature Expert Panel. Since 2014 he has acted as a consultant to NRGD, the Netherlands Register for Court Experts.

Since 2017 he has been on National Crime Agency MCIS register of expert witnesses and has carried out many instructions for the NCA and Regional Organised Crime Units.

He is on the Editorial Boards of *Computer Fraud and Security Bulletin, Secure Computing, Digital Investigation* and *International Journal of Digital Crime and Forensics* and has served on the conference committees of a number of academic symposia, including RAID (Recent Advances in Intrusion Detection) FIRST2000 Conference, Chicago, EICAR 2005 and 2007, DIGEV 2005 and WDFIA 2007, 2008 2009 and 2010, and DFRWS-EU from its inception

Previous Career / Information Security Consultancy

Peter Sommer read law at Oxford and spent thirteen years as a book publisher.

He has always had a subsidiary career as author and journalist. His interest in computing dates from the late 1960s when he was a guinea pig in work carried out by the late Dr Christopher Evans at the National Physical Laboratory.

He was among the first generation of writers on micro-computers in the mid-1970s and entered professional computing via electronic publishing.

As an electronic publisher he set up a variety of services on Prestel, the pioneering public access database run by British Telecom, and on TOPIC, the information system of the London Stock Exchange and has also been an external Information provider for Reuters and Extel. In the run-up to the Big Bang changes in the London markets he set up a prototype investment exchange for over-the-counter securities. He has also carried out a wide range of consultancy assignments involving the commercial exploitation of new technologies and system assessment.

In 1985 he wrote, under the pseudonym, Hugo Cornwall, the best- selling *Hacker's Handbook* which was in the Sunday Times list for seven weeks and finally went into four editions, of which Mr Sommer wrote the first three. The book was about accessing the online world from personal computers and computer security. From then on Mr Sommer moved into computer security consultancy, initially as a freelance for two leading UK security companies and then as a founder-director of Data Integrity where he was Technical Director responsible for surveys. He left Data Integrity in March 1989 and since then worked principally for leading loss adjusters and corporate security companies, and under the umbrella of his own company, a specialist London-based computer security consultancy Virtual City Associates which provides services to insurers, lawyers and corporate security companies world-wide. He helped develop one the earliest cyber crime insurance polices, the SPP, which was a computer-related consequential loss/business interruption cover, and has also carried out surveys for the Bankers Blanket Bond and Computer Crime policies as well as computer-related special covers. Survey subjects have included a major international payment system, a major global securities trading system, a large securities settlement service, an Internet-only bank and two fast- growing Stock Exchanges, advising insurers initially on formats for cover as well as later carrying out the risk analysis for the policy selected. More routine assignments have included insurance surveys / loss adjustment support on many large commercial and state-owned financial institutions in Europe, South America and South East Asia.

Non-insurance assignments have included advising a major UK-based international conglomerate operating in nearly sixty countries and about to install a series of complex local and wide areas networks, a large UK retailer with a suspected unwanted intruder on its internal computer networks, and an extended risk management survey for European-based securities settlement service. Civil instructions have involved questioned emails and alleged hacking to obtain access to bitcoin wallets.

The *Hackers's Handbook* was followed in 1988 by *DataTheft* and *The Industrial Espionage Handbook* was published in October 1999. His most recent publication is an ebook. *Digital Evidence Handbook,* available via Amazon/Kindle. Professor Sommer regularly appears in television and radio programs and at conferences for the commercial, academic, law enforcement and government communities. Professor Sommer has been a Member of the British Computer Society since 1988 and has served on its Legal Affairs Committee. He became a Fellow in 2014.

Academic Interests

Peter Sommer became a Visiting Fellow in what was the Information Systems Department at the London School of Economics since 1994 and was a Visiting Professor 2008-2011. With Dr Jim Backhouse he developed and taught a range of Information System Security courses, with their emphases on social science, management, law and policy. The aim has been to balance theory and analysis with the problems of implementation and is in contrast to the more usual approach which consists largely of finding technical solutions to what are wrongly perceived as purely technical problems.

He has examined at doctoral level at Cranfield and Oxford Brookes Universities.

Academic interests include: Computer-related Crime, Computer Misuse, White Collar Crime, Frauds, Industrial Espionage, Methods of Information Security research including case material collection and evaluation, Legal Implications of Information Security, Methods of Risk Analysis, Insurance of Computer-related risks, ECommerce, Digital Signatures, Issues of Contingency Planning / Disaster Recovery, Electronic Publishing, Internet control issues, Intellectual Property.

In 2003-4, he was expert member of UK DTI *Foresight* Project *Cyber Trust and Crime Prevention* (http://www.foresight.gov.uk/cybertrust.html). Other funded research included the forensic aspects of identity systems under FIDIS (www.fidis.net) which was a European Commission-funded Network of Excellence and PRIME (http://www.prime-project.eu.org/) which was a European Commission Framework 6 Integrated Project on Privacy Enhancing Technologies (Reference Group member). Together with LSE colleagues he provided "Best Practice" consultancy to a syndicate of central government departments and UK clearing banks and to APACS. In September 2000 a LSE team headed by Professor Sommer was awarded a contract by the UK's Financial Services Authority to provide advice on consumer use of e-commerce facilities in the purchase of financial products such as banking, insurance, pensions, savings, and share-dealing to assist in the development of a suitable regulatory regime.

In 2009 Professor Sommer won a contract from the UK National Audit Office to support its examination of Internet Crime,

In February 2006 Mr Sommer was appointed a Visiting Research Fellow at the Faculty of Mathematics and Computing, Open University, and was later elevated to Visiting Reader. He was the Course Consultant for a Masters' course module on Computer Investigations and Forensics. In 2012 he joined the Cyber Security Centre at De Montfort University as Visiting Professor.

He is now Professor of Digital Forensics at Birmingham City University.

Public Policy Work

In December 1998 Peter Sommer was appointed Specialist Advisor to the House of Commons Select Committee on Trade and Industry to support their inquiry into ecommerce. This has produced four published Reports. Seventh Report (HC 187); "Building confidence in Electronic Commerce" . Tenth Report of Session (HC 648), "Electronic Commerce", Fourteenth Report of Session (HC 862), "Draft Electronic Communications Bill" , Eighth Report of Session (HC66): UK Online Reviewed: The First Annual Report Of The E-Minister And E-Envoy.

In December 2000 Professor Sommer and colleagues were awarded a European Commission contract to carry out the Intermediate Evaluation of the EC Internet Action Plan (on illegal and harmful content on the Internet). He is on the Advisory Council of the Foundation for Information Policy Research, is a Member of the Information Assurance Advisory Council and has Observer status at EURIM.

Between July 2003 and March 2009 he was a member of the Scientific Advisory Panel on Emergency Response (SAPER) run by the Government's Chief Scientific Advisor. (SAPER is the predecessor of SAGE). In 2008 he was appointed to the Digital Forensics Specialist Group which advises the Forensic Science Regulator.

In 2009, with colleagues in the LSE's Public Engagement Network, he authored a study of the UK Government's *Interception Modernisation Program*.

In February 2010 he took part in the work of the United Nations Counter-Terrorism Implementation Task Force (http://www.un.org/terrorism/internet.shtml).

In November 2010 he provided written and oral evidence to the Commons Science and Technology Select Committee's enquiry into *Scientific advice and evidence in emergencies* and in November 2011 to its enquiry into *Malware and cybercrime*

In 2011, with Ian Brown of the Oxford Internet Institute he wrote *Reducing Systemic Cyber Security Risk* for the Organisation of Economic Co-operation and Development (OECD), part of its Future Global Shocks Program.

In 2013 he provided written and oral evidence to the Joint Committee examining the draft Communications Data Bill and in the same year to the Commons Home Affairs Select Committee investigation of e-Crime. In 2014 he gave written and oral evidence to the Intelligence and Security Committee of Parliament in their inquiry into Privacy and Security. He also given evidence to the Home Affairs Select Committee, the All Party Privacy Group and the TOEIC APPG.

In 2014 he was invited to join the Home Office Digital Signature Expert Panel within the Office of Security and Counter Terrorism Communications Capability Development program

Between November 2015 and February 2016 he acted as a Specialist Advisor to the Lords and Commons Joint Committee scrutinizing the Draft Investigatory Powers Bill.

In 2009 and again in 2017 he was part of the team that carried out an external audit of the Hotline of the Internet Watch Foundation.

Selected Publications

Under the pseudonym "Hugo Cornwall":
The Hacker's Handbook, Random-Century, 1985, 1986, 1988, 1989.
DataTheft, Heinemann Professional, 1987, Mandarin Paperbacks, 1990.
The Industrial Espionage Handbook , Century 1991, Ebury Press, 1992.
Under own name:
The PC Security Guide 1993-1994, Elsevier, 1993. *Why Legislation is the not the answer; the limits of the Law* Compacs 91, 15th International Conference on Computer Audit, Control and Security, IAA.

Computer Forensics: an Introduction Compsec '92, Elsevier.
Computer-Aided Industrial Espionage Compsec '93, Elsevier.
Industrial Espionage: Analysing the Risk Compsec '94, Elsevier.
Various practitioner-orientated articles appear passim in *Computer Fraud and Security Bulletin,* published by Elsevier and *Virus News International* and *Secure Computing,* published by West Coast Publishing.
The computer security sections of *Handbook of Security* and *Purchasing and Supply Guide to Guide to IT* both published by Croner.
Imaged documents code,. Computer Fraud & Security, Apr 1996.
England ponders trade secrets law, Computer Fraud & Security, Jan 1998
Investigating Computer Crime (book review) Computer Fraud & Security, Sep 1997.
Fraud Watch: A Guide for Business - Ian Huntington and David Davies (book review). Computer Fraud & Security, Apr 1995.
Information Warfare: Chaos on the Electronic Superhighway - Author: Winn Schwartau (book review). Computer Fraud & Security, Jun 1995.
Computer-Related Risks - Author: Peter G Neumann. (book review) Computer Fraud & Security, Jul 1995
Downloads, Logs and Captures: Evidence from Cyberspace Journal of Financial Crime, October, 1997, 5JFC2 138-152;
Intrusion Detection Systems as Evidence RAID 98 Conference, Louvain-la-Neuve, Belgium; also in *Intrusion detection systems as evidence*, Computer Networks, Volume 31, Issues 23-24, 14 December 1999, Pages 2477-2487.
Legal Reliability in Large Scale Distributed Systems IEEE Symposium on Reliable Information Systems, COAST/Purdue University, 1998;
Digital Footprints: Assessing Computer Evidence Criminal Law Review (Special Edition, December 1998, pp 61-78)
Co-author: *CyberCrime: Risk and Response*. International Chamber of Commerce ICC Publication 621, 1999
Sommer, P: *Evidence in Internet Paedophilia Cases* Computer and Telecommunications Law Review, Vol 8 Issue 7; [2002] CTLR, pp 176-184
Sommer, P: *Evidence in Internet Paedophilia Cases; a case for the Defence* in "Policing Paedophiles on the Internet" ed McVean & Spindler, New Police Bookshop for the John Grieve Centre, 2003.
Computer Forensics Education , Yasinac, Erbacher, Marks, Pollitt, Sommer, IEEE Security & Privacy Vol 1 No 4 p 15 , July 2003;
The future for the Policing of Cybercrime Computer Fraud & Security Bulletin, January 2004, pp 8-12
Co-author: *CyberCrime: Risk and Response*. International Chamber of Commerce ICC Publication 621, 1999
Cybercrime (co-author) and *Computer Aids* chapters in *Fraud: Law, Procedure and Practice*, Lexis-Nexis / Butterworths, 2004, 2009, 2013
The challenges of large computer evidence cases Digital Investigation Vol 1 Issue 1 2004 16-17,
Digital Evidence: a Guide for Directors and Corporate Advisors, Information Assurance Advisory Council, September 2005., revised edition November 2008
Two Computer Misuse Prosecutions Computers and Law Vol 16 issue 5, 2006
Criminalising Hacking Tools Digital Investigation Vo 3 Issue 3 2006 68-72
Meetings Between Experts: a route to simpler fairer trials Digital Investigation diin.2008.11.002

Forensic science standards in fast-changing environments Science and Justice 50:11, 12-17, March 2010
Reducing Systemic Cyber Security Risk, OECD, Paris, January 2011.
http://www.oecd.org/dataoecd/3/42/46894657.pdf

Police Powers to Hack CTLR, 2012
Digital Surveillance, Open Rights Group, May 2013, 2 sections
Two *Guardian Comment is Free* pieces on GCHQ oversight:
http://www.theguardian.com/commentisfree/2013/aug/02/whos-watching-gchq and
http://www.theguardian.com/commentisfree/2013/aug/02/whos-watching-gchq
Stronger Oversight of GCHQ – How?
http://www.opendemocracy.net/ourkingdom/peter-sommer/stronger-oversight-of-gchq-how
Big Data and privacy: DI commentary, Digital Investigation, 2015 pp 101-103, https://doi.org/10.1016/j.diin.2015.10.001
Accrediting digital forensics: what are the choices? Digital Investigation, Vol 25, June 2018 116-120 https://doi.org/10.1016/j.diin.2018.04.004
Digital Evidence Handbook Amazon / Kindle, April 2017.

Reforming the Computer Misuse Act 1990 (co-author) CLRNN 2020
http://www.clrnn.co.uk/publications-reports

Website

www.pmsommer.com: