BIBLIOGRAPHY

BOOKS

Akdeniz, Y, *Internet Child Pornography and the Law: National and International Responses*, Ashgate: 2008.

Arkin, S (ed), *Prevention and Prosecution of Computer and High Technology Crime*, Matthew Bender, 1990.

Arlidge, A and Parry, J, *Arlidge and Parry on Fraud*, Sweet & Maxwell, 2005.

Ashworth, A, and Horder, J. *Principles of Criminal Law*, 7th edn, Oxford University Press, 2009.

Ashworth, A and Redmayne, M, *The Criminal Process*, 4th edn, Oxford University Press, 2010.

Ashworth, A, Macdonald, A, and Emmerson, B, *Human Rights and Criminal Justice*, 3rd edn, Sweet & Maxwell, 2012.

Bantekas, I and Nash, S, *International Criminal Law*, Routledge Cavendish, 2003. Barrett, N:
(a) *Digital Crime: Policing the Cybernation*, Kogan Page, 1997.
(b) *Traces of Guilt*, Corgi, 2009.

Bently, L and Sherman, B, *Intellectual Property Law*, 4th edn, Oxford, 2014.

Bequai, A, *Technocrimes*, Lexington Books, 1987.

Blackstone's Criminal Practice, Oxford University Press, 2016.

Boister, N, *An Introduction to Transnational Criminal Law*, Oxford University Press: 2012.

Boni, WC, and Kovacich, GL, *I-Way Robbery: Crime on the Internet*, Butterworth, 1999.

Brenner, S, *Cyberthreats and the Decline of the Nation-State*, Routledge: 2014.

Casey, E, *Digital Evidence and Computer Crime*, 3rd edn, Academic Press, 2011.

Cassese, A, et al, *International Criminal Law*, 3rd edn, Oxford University Press, 2013.

Clifford, R, *Cybercrime: The Investigation, Prosecution and Defence of a Computer-related Crime*, 3rd edn, Carolina Academic Press, 2011.

Clough, J., *Principles of Cybercrime*, Cambridge University Press: 2010.

Coppel, P (ed), *Information Rights: Law and Practice*, 4th ed, Hart Publishing, 2014.

Cornwall, H, *Data Theft*, Mandarin, 1990.

Coupland, D, *Microserfs*, Flamingo, 1995.

Delmas-Marty, M and Spencer, JR (eds), *European Criminal Procedures*, Cambridge University Press, 2002.

Duff, R and Green, S (eds), *Defining Crimes*, Oxford University Press, 2005.

Endicott, T., *Vagueness in Law*, Oxford University Press, 2000.

Farr, R, *The Electronic Criminals*, Fontana, 1977.

Furnell, S, *Cybercrime: Vandalizing the Information Society*, Pearson, 2002.

Gibson, W, *Neuromancer*, HarperCollins, 1984.

Gillespie, A, *Child Pornography: Law and Policy*, Routledge-Cavendish, 2011.

Glenny, M, *DarkMarket: Cyberthieves, CyberCops, and You*, The Bodley Head, 2011

Gurry on Breach of Confidence, 2nd ed., OUP, 2012.

Grabosky, P, Smith, RG, and Dempsey, G, *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, 2001.

Grady, MF and Parisi, F, *The Law and Economics of Cybersecurity*, Cambridge, 2006.

Grewlich, K, *Governance in Cyberspace*, Kluwer Law International, 1999.

Hafner, K and Markoff, J, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon and Schuster, New York, 1991.

Harfield, C and Harfield, K, *Covert Investigations: A Practical Guide for Investigators*, 3rd Edn, Oxford University Press, 2012.

Hirst, M, *Jurisdiction and the Ambit of the Criminal Law*, Oxford University Press, 2003.
Hollinger, RC (ed), *Crime, Deviance and the Computer*, Dartmouth, 1997.
The Honeynet Project, *Know Your Enemy: Learning about Security Threats*, 2nd edn, Addison-Wesley Professional, 2004.
Janssens, C., *The Principle of Mutual Recognition in EU Law*, OUP, 2013.
Jewkes, Y (ed), *Dotcons: Crime, Deviance and Identity on the Internet*, Willan, 2003.
Jewkes, Y, and Yar, M, *Handbook of Internet Crime*, Willan, 2009.
Jordan, T and Taylor, PA, *Hactivism and Cyberwars: Rebels with a Cause*, Routledge, 2004.
Keefe, P, *Chatter: Dispatches from the Secret World of Global Eavesdropping*, Random House, 2005.
Kelman, A and Sizer, R, *The Computer in Court*, Ashgate, 1982.
Koops, B-J and Brenner, S (eds), *Cybercrime Jurisdiction: A Global Survey*, TMC Asser Press, 2006.
Latham, E, *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, New Press, 2003.
Lessig, L, *Code and Other Laws of Cyberspace*, Basic Books, New York, 2000.
Levy, S, *Hackers*, Penguin, 1984.
Lilley, P, *Hacked, Attacked & Abused*, Kogan Page, 2002.
Littman, J, *The Watchman: The twisted life and crimes of serial hacker Kevin Poulson*, Little, Brown & Co, 1997.
Mason, S., (ed), *Electronic Evidence*, 3rd ed., LexisNexis, 2012.
Marsden, C., *Internet Co-Regulation*, Cambridge University Press, 2011.
McKay, S., *Covert Policing: Law and Practice*, 2nd edn, OUP, 2015.
McKnight, G, *Computer Crime*, Michael Joseph, 1973.
Millard, C., *Cloud Computing Law*, OUP, 2013.
Millwood Hargrave, A and Livingstone, S, *Harm and Offence in Media Content*, Intellect 2006.
Mitnick, K and Simon, WL, *Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*, Hungry Minds, 2005.
Naughton, J, *A Brief History of the Future*, Phoenix, 2000.
Naylor, R, *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*, Cornell University Press, 2004.
Newman, G and Clarke, R, *Superhighway Robbery: Preventing e-Commerce Crime*, Willan Publishing, 2003.
Ormerod, D, and Laird, K, *Smith & Hogan Criminal Law*, 14th edn, Oxford University Press, 2015.
Packer, H, *The Limits of the Criminal Sanction*, Stanford University Press, 1969.
Parker, D,
(a) *Crime by Computer*, Charles Scribner's Sons, 1976.
(b) *Fighting Computer Crime: A New Framework for Protecting Information*, Wiley, New York, 1998.
Powles, S, Waine, L, and May, R and, *Criminal Evidence*, 6th edn, Sweet & Maxwell, 2015.
Price, M and Verhulst, S, *Self-Regulation and the Internet*, Kluwer Law International, 2005.
Raymond, E, *The New Hacker's Dictionary* 3rd edn, MIT Press, 1996.
Reed, C,
(a) *Internet Law: Text and Materials*, 2nd edn, Cambridge University Press, 2004.
(b) *Making Laws for Cyberspace*, Oxford University Press, 2012
Richardson, M, *Cyber Crime: Law and Practice*, Wildy, Simmonds and Hill Publishing, 2014.
Roberts, P and Zuckerman, A, *Criminal Evidence*, 2nd edn, Oxford University Press, 2010.
Schmitt, M, (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013
Schneier, B, *Secrets and Lies: Digital Security in a Networked World*, Wiley, 2000.
Shapiro, C and Varian, H, *Information Rules: A Strategic Guide to the Network Economy*, HBS Press, 1998.
Shotton, M, *Computer Addiction?: A Study of Computer Dependency*, Taylor & Francis, 1989.

Sieber, U, *The International Handbook on Computer Crime*, Wiley, 1986.
Simester, AP, Spencer, JR, Sullivan, GR and Virgo GJ, *Criminal Law: Theory and Doctrine* 5th edn, Hart, 2013.
Smith, ATH, *Property Offences*, Sweet & Maxwell, 1994.
Smith, R, Grabosky, P, and Urbas, G, *Cyber Criminals on Trial*, Cambridge University Press, 2004.
Sofaer, A and Goodman, S, *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Institution, 2001.
Spitzner, L, *Honeypots: Tracking Hackers*, Addison-Wesley, 2002.
Sterling, B, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Penguin Books, 1994.
Stoll, C, *Cuckoo's Egg*, Pocket Books, 1998.
Summers, S., et al., *The Emergence of EU Criminal Law: Cyber crime and the regulation of the Information Society*, Hart Publishing, 2014.
Tapper, C, *Computer Law*, 4th edn, Longman, 1989.
Tapper, C, *Cross & Tapper on Evidence*, 12th edn, Oxford University Press, 2010.
Taylor, M and Quayle, E, *Child Pornography: An Internet Crime*, Brunner-Routledge, 2003.
Taylor, P, *Hackers: Crime and the Digital Sublime*, Routledge, 1999.
Thomas, D and Loader, B (eds), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, 2000.
Turkle, S, *Life on the Screen: Identity in the Age of the Internet*, Simon & Schuster, 1997.
Wacks, R, *Personal Information, Privacy and the Law*, Clarendon Press, 1989.
Walden, I, *Telecommunications Law and Regulation*, Oxford University Press, 2012.
Wall, DS,
(a) (ed) *Crime and the Internet: Cybercrimes and Cyberfears*, Routledge, 2001.
(b) (ed) *Cyberspace Crime*, Dartmouth, 2003.
(c) *Cybercrime: The Transformation of Crime in the Information Age*, Polity, 2007.
Wall, DS, and Williams, M, (ed) *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*, Routledge, 2014
Warren, P and Streeter, M, *Cyber Alert: How the World is Under Attack from a New Form of Crime*, Vision Publishing, 2005.
Wasik, M, *Crime and the Computer*, Clarendon Press, 1991.
Westby, JC, *International Guide to Combating Cybercrime*, American Bar Association, Chicago, 2003.
Whiteside, T, *Computer Capers*, Sidgwick and Jackson, 1979.
Wilding, E, *Computer Evidence*, Sweet & Maxwell, 1997.
Williams, V, *Surveillance and Intelligence Law Handbook*, Oxford University Press, 2006.

ARTICLES

Akdeniz, Y, 'The regulation of pornography and child pornography on the Internet' 1997 (1) *The Journal of Information Law and Technology*, available at: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1/>.
Anderson, R, Needham, R, and Shamir, A, 'The steganographic file system', pp 73–82, in Ausmith, D (ed), *Information Hiding*, Springer-Verlag, 1998.
Anderson, R. and others, 'Measuring the Cost of Cybercrime', pp. 265-300, in *The Economics of Information Security and Privacy*, Pt. IV, 2013
Andrews S, 'Who Holds the Key?—A comparative study of US and European encryption policies', 2000 (2) *The Journal of Information, Law and Technology* <http://elj.warwick.ac.uk/jilt/00-/andrews.html>.
Armstrong, HL and Forde, PJ, 'Internet anonymity practices in computer crime', *Information Management & Computer Security*, vol 11, No 5, 2003.
Ashworth, A, and Blake, M, 'The presumption of innocence in English criminal law' [1996] Crim LR 306.

Bacigalupo, E, 'The use of technical means in interception and surveillance of private communications', pp 131–42, in Militello, V and Huber, B, (eds) *Towards a European Criminal Law Against Organised Crime*, Edition Iuscrim, 2001.

Baldwin, R and Hawkins, K, 'Discretionary justice: Davis reconsidered' [1984] *Public Law* 570.

Barlow, JP, 'Crime and puzzlement: In advance of the law on the electronic frontier', pp 1–24, *Whole Earth Review*, 68, Fall 1990.

Baron, R, 'A critique of the international cybercrime treaty', pp 263–278, *CommLaw Conspectus* 10 (2002).

Barton, P and Nissanka, V, 'Cyber-crime—criminal offence or civil wrong?' pp 401–5, *Computer Law and Security Report*, vol 19, No 5, 2003.

Bazelon, D, Choi, Y, and Conaty, J, 'Computer Crimes', 43 *American Criminal Law Review* 259, 2006.

Bell, E, 'The Prosecution of Computer Crime', pp 308–25, *Journal of Financial Crime*, vol 9, No 4, 2002.

Bennett, D., "The challenges facing computer forensic investigations in obtaining information from mobile devices for use in criminal investigations", 20 August 2011, available at <www.forensicfocus.com>.

Birnhack, MD, and Elkin-Koren, N, 'The invisible handshake: The reemergence of the state in the digital environment', 8 *Va JL & Tech* 6, 2003.

BloomBecker, JJB, 'Computer crime and abuse', pp 34–41, *The EDP Auditor Journal*, II, 1990.

Boehm, F. and M. Cole, "Data Retention after the judgement of the Court of Justice of the European Union", available at <www.janalbrecht.eu/>

Bowden, C, 'The US surveillance programmes and their impact on EU citizens' fundamental rights', Report for the European Parliament, 2013

Brenner, S,

(a) 'Is there such a thing as "virtual crime"', 4 *California Criminal Law Review* 1, 2001.

(b) 'In defense of cyberterrorism', 2 *The University of Illinois Journal Of Law, Technology & Policy* 1, 2002 (with Marc D Goodman).

(c) 'Organised cybercrime? How cyberspace may affect the structure of criminal relationships', *North Carolina Journal of Law and Technology*, vol 4, No 1, Fall 2002.

(d) 'Transnational evidence-gathering and local prosecution of international cybercrime', 20 *The John Marshall Journal of Computer and Information Law* 347, 2002 (with Joseph Schwerha IV).

(e) 'Toward a criminal law for cyberspace: Distributed security', 10 *BU J Sci & Tech L* 2, 6–11, 2004.

(f) 'Distributed security: Moving away from reactive law enforcement', *International Journal of Communications Law and Policy*, Special Issue Cybercrime, Spring 2005.

(g) 'Defining cybercrime: A review of state and federal law', pp 13–95, in Clifford, R, *Cybercrime: The Investigation, Prosecution and Defence of a computer-related crime*, 2nd edn, Carolina Academic Press, 2006.

(h) 'Law, Dissonance, and Remote Computer Searches', *North Carolina Journal of Law & Technology*, 14(1) (2012), 43.

Brenner, S and Goodman, M, 'Cybercrime: The need to harmonize national penal and procedural laws', International Society for the Reform of Criminal Law 16th Annual Conference Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice, 2002.

Brenner, S and Koops, B-J, 'Approaches to cybercrime jurisdiction', 4 *Journal of High Technology Law* 1, 2004.

Broucek, V and Turner, P, 'Intrusion detection: Issues and challenges in evidence acquisition', pp 149–64, *International Review of Law Computers & Technology*, vol 18, No 2, 2004.

Burden, K and Palmer, C, 'Cyber crime—A new breed of criminal?', pp 222–7, *Computer Law and Security Report*, vol 19, No 3, 2003.

Calabresi, G, and Douglas Melamud, A, "Property Rules, Liability Rules and Inalienability: One View of the Cathedral" [1971], 85 *Harvard law Review*. 1089.

Campbell, D., "GCHQ and me: My life unmasking British eavesdroppers', 3 August 2015, available at www.firstlook.org/theintercept/.

Cangemi, D, 'Procedural law provisions of the Council of Europe Convention on Cybercrime', pp 165–71, *International Review of Law Computers & Technology*, vol 18, No 2, 2004.

Chandler, JA,

(a) 'The changing definition and image of hackers in popular discourse', pp 229–51, *International Journal of the Sociology of Law*, vol 24, No 2, 1996.

(b) 'Security in cyberspace: Combating distributed denial of service attacks', 1 *University of Ottawa Law and Technology Journal* 231, 2003–04.

Charney, S, 'Combating cybercrime: A public-private strategy in the digital environment', paper written for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 18–23 April 2005, Bangkok, Thailand.

Christie, AL, 'Should the law of theft extend to information?', pp 349–60, *The Journal of Criminal Law*, vol 69, No 4, 2005.

Clayton, R, 'Anonymity and traceability in cyberspace', University of Cambridge, Computer Laboratory, Technical Report, UCAM-CL-TR-653, November 2005. Available at <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html>.

Conte, A, 'Crime and terror: New Zealand's criminal law reform since 9/11', pp 635–64, *New Zealand Universities Law Review*, vol 21, No 4, 2005.

Cormack, A, 'Logfiles', JANET Guidance Note GD/NOTE/008, June 2004, available at <http://www.ja.net/services/publications/technical-guides/logfiles.pdf>. Cross, JT,

(a) 'Trade secrets, confidential information, and the criminal law', 36 *McGill Law Journal*, 524, 1991.

(b) 'Protecting confidential information under the criminal law of theft and fraud', 11 *Oxford Journal of Legal Studies* 264, 1991.

Davies, CR, 'Protection of intellectual property—A myth?, pp 398–410, *The Journal of Criminal Law*, vol 68, pt 5, October 2004.

Davies, L, 'Packets and bits: Forensic investigation on the Internet—Paper trails and coolie crumbs', *The Litigator* 35, 1997.

Davis, RH, 'Social network analysis: An aid in conspiracy investigations', *FBI Law Enforcement Bulletin* pp 11–19, 1981.

Decroos, M, 'Criminal jurisdiction over transnational speech offenses', pp 365–400, *European Journal of Crime, Criminal Law and Criminal Justice*, vol 13, No 2005.

de Hert, P. and M. Kopcheva, 'International mutual legal assistance in criminal law made redundant: A comment on the Belgium Yahoo! case' (2011) *Computer Law and Security Review*, 27.

Demeyer, K., Lievens, E. and Dumortier, J. (2012), "Blocking and Removing Illegal Child Sexual Content: Analysis from a Technical and Legal Perspective". *Policy & Internet*, 4: 1–23.

Denning, D, 'Cyberterrorism: The logic bomb versus the truck bomb', *Global Dialogue*, Autumn, pp 29–37, 2000.

Denning, D and Baugh, W, 'Hiding crimes in cyberspace', pp 105–31, in Thomas, D and Loader, B (eds), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, 2000.

Douglas-Scott, 'The rule of law in the European Union—Putting security into the area of freedom, security and justice', pp 219–42, 29 *European Law Review*, 2004.

Duff, RA, 'Subjectivism, objectivism and criminal attempts', pp 19–44, in *Harm and Culpability* (Simester, AP and Smith, ATH, eds), Clarendon Press, 1996.

Ellison, L and Akdeniz, Y, 'Cyber-stalking: The regulation of harassment on the Internet', in Walker, C (ed), *Crime, Criminal Justice and the Internet* (special edition, *Criminal Law Review*), Sweet & Maxwell, London, 1998.

Endeshaw, A, 'Theft of information revisited' *Journal of Business Law*, 187, 1997.

Esposito, LC, 'Regulating the Internet: The new battle against child pornography', *Case Western Reserve Journal of International Law*, 1998, vol 30, No 2/3, 541.

Feiler, L., "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", *European Journal of Law and Technology*, Vol. 1,Issue 3, 2010.

Flanagan, A, 'The law and computer crime: Reading the script of reform', pp 98–117, *International Journal of Law and Information Technology*, vol 13, No 1, 2005.

Fletcher, M, 'Extending "indirect effect" to the third pillar: the significance of *Pupino*?, pp 863–77, 30 *European Law Review*, December 2005.

Forest Wolfe, D, 'The Government's right to read: Maintaining state access to digital data in the age of impenetrable encryption', *Emory Law Journal* 711, 2000.

Fournier, R., and others, "Comparing pedophile activity in different P2P systems", *Social Sciences* 2014, 3, 314–325.

Freedman, CD,

(a) 'Criminal misappropriation of confidential commercial information and cyberspace: Comments on the issues', pp 147–62, 13 *International Review of Law, Computers and Technology*, 1999.

(b) "*The New Law of Criminal Organizations in Canada*" (2007) 85(2) Canadian Bar Review 171

Froomkin, M, 'It came from Planet Clipper: The battle over cryptographic key "escrow"', *U Chi L Forum* 15, 1996.

Gane, C, and Mackarel, M, 'The admissibility of evidence obtained from abroad into criminal proceedings: The interpretation of mutual legal assistance treaties and use of evidence irregularly obtained' (1996) 4 Eur J Crime, Crim L & Crim Just 98, 116

Garrie, D, Armstrong, M, and Harris, D, 'Voice over Internet Protocol and the Wiretap Act: Is your conversation protected?' p 97, *Seattle University Law Review*, vol 29, 2005.

Gillespie, AA,

(a) 'Children, chatrooms and the law', [2001] *Criminal Law Review*, 435.

(b) 'The Sexual Offences Act 2003: (3) Tinkering with 'child pornography', [2004] *Criminal Law Review*, 361.

(c) 'Child pornography: Balancing substantive and evidential law to safeguard children effectively from abuse', pp 29–49, *International Journal of Evidence & Proof*, vol 9, No 1, 2005.

(d) 'Restricting access to the internet by sex offenders' *Int J Law Info Tech* (2011) 19 (3): 165-186.

Goldstone, D, and Shave, B, 'International dimensions of crimes in cyberspace', 22 *Fordham International Law Journal* 1924, 1999.

Goodman, MD, 'Why the police don't care about computer crime', 10 *Harvard Journal of Law and Technology* 465, 1997.

Grabosky, P, 'Virtual criminality: Old wine in new bottles', 10 *Social & Leg Studies* 243, 2001.

Grabosky, PN and Smith, R, 'Digital crime in the twenty-first century', pp 8–26, *Journal of Information Ethics*, Spring 2001.

Grover, D, 'Dual encryption and plausible deniability', pp 37–40, *Computer Law and Security Report*, vol 20, No 1, 2004.

Haggerty, Karran, Lamb and Taylor, 'A framework for the forensic investigation of unstructured email relationship data', *International Journal of Digital Crime and Forensics*, 3(3), 1-18, 2011.

Haines, J and Johnstone, P, 'Global cybercrime: New toys for the money launderers', pp 317–25, *Journal of Money Laundering Control*, vol 2, No 4.

Hammond, RG, 'Theft of Information', pp 252–64, *Law Quarterly Review*, vol 100, April 1984.

Hatcher, M, McDannell, J, and Ostfeld, S, 'Computer crimes', 36 *American Criminal Law Review*, 397.

Hirst, M, 'Cyberobscenity and the ambit of English criminal law', *Computers and Law*, vol 13, No 2, 2002.

Hoey, A, 'Techno-cops: Information technology and law enforcement', pp 69–90, *International Journal of Law and Information Technology*, vol 6, No 2, 1996.

Hofmeyr, K, 'The problem of private entrapment' [2006] Crim LR 319.

Hollinger, RC,

(a) 'Hackers: Computer heroes or electronic highwayman?', pp 6–17, *Computers and Society*, 21, 1991.

(b) 'Crime by computer: Correlates of software piracy and unauthorized account access', pp 2–12, *Security Journal*, 4, 1993.

Hosein, I, 'The sources of laws: Policy dynamics in a digital and terrorized world', pp 187–99, *The Information Society*, vol 20, No 3, 2004.

Hosein, I and Pascuual, A, 'Understanding traffic data and deconstructing technology-neutral regulations', March 2002, available at <http://www.it46.se/docs/papers/unece-latest-escuderoa-hoseini.pdf>.

International Journal of Communications Law and Policy, Special Issue on Cybercrime, Issue 9, Part II, Autumn 2004.

Jarvie, N, 'Control of cybercrime—Is an end to our privacy on the Internet a price worth paying?' *Computer and Telecommunications Law Review*, Part 1: 76–81 (9(3)), Part 2: 110–15 (9(4)), 2003.

Jordan, T and Taylor, P, 'A sociology of hackers', pp 757–80, *Sociological Review*, November 1998.

Kabay, M, 'Studies and surveys of computer crime', 2001, available from <http://www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf>.

Karnow, C, 'Launch of warning: Aggressive defense of computer systems', pp 87–102, *Yale Journal of Law and Technology*, Fall 2004–05.

Katyal, NK,

(a) 'Criminal law in cyberspace', 149 *University of Pennsylvania Law Review* 1003, 2001.

(b) 'The dark side of private ordering', pp 193–217 in Grady, MF and Parisi, F, *The Law and Economics of Cybersecurity*, Cambridge, 2006.

Kelman, A, 'The regulation of virus research and the prosecution for unlawful research?' Commentary, *The Journal of Information, Law and Technology*, 1997(3), <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_3/kelman1/>.

Kenneally, E, 'The Internet is the computer: The role of forensics in bridging the digital and physical divide', pp 41–4, *Digital Investigation* 2, 2005.

Kenneally, E and Brown, C, 'Risk sensitive digital evidence collection', *Digital Investigation* (2005) 2, 101–19.

Kent, G, 'Sharing Investigation-specific Data With Law Enforcement - An International Approach', (2014), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413>.

Kerr, I and Gilbert, D, 'The role of ISPs in the investigation of cybercrime', pp 163–72, Chapter 20 in *Information Ethics in the Electronic Age* (Mendina, T and Britz, J eds), McFarland Press, 2004.

Kerr, O,

(a) 'Cybercrime's scope: interpreting "access" and "authorization" in computer misuse statutes', *New York University Law Review* 1596, 2003.

(b) 'Lifting the "fog" of Internet surveillance: How a suppression remedy would change computer crime law', 54 *Hastings Law Journal* 805, 2003.

(c) 'Digital evidence and the new criminal procedure', *Columbia Law Review*, January 2005.

(d) 'Fourth Amendment Seizures of Computer Data', *Yale Law Journal*, 119 (2010), 700.

Koops, BJ,

(a) 'Commanding decryption and the privilege against self-incrimination', pp 431–445, in *New Trends in Criminal Investigation: Volume 2*, (eds Breur, Kommer, Nijboer and Reijntjes), Intersentia, 2000.

(b) 'Should ICT regulation be technology-neutral?', pp 77–108, in Koops, B-J et al (eds), *Starting Points for ICT Regulation*, TMC Asser Press, 2006.

Kosta, E, "The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection", (2013) 10:3 *SCRIPTed* 339

Kshetri, N, 'The simple economics of cybercrimes', pp 33–9, *IEEE Security and Privacy*, vol 4, Issue 1, January/February 2006; available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=881421>.

Lanham, D, 'Larsonneur revisited' [1976] Crim LR 276.

Levi, M, 'The organisation of serious crimes', pp 878–913, *The Oxford Handbook of Criminology*, 3rd edn, Oxford University Press, 2002.

Lewis, BC, 'Prevention of computer crime amidst international anarchy', 41 *American Criminal Law Review* 1353, 2004.

Lewis, O, 'Information security & electronic eavesdropping—a perspective', pp 165–8, *Computer Law and Security Report*, vol 7, No 4, 1991.

Lipson, HF, *Tracking and tracing cyber-attacks: technical challenges and global policy issues*, CERT Coordination Center, Special Report CMU/SEI-2002-SR-009, November 2002 at 10, <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5831>.

Loof, R, 'Obtaining, adducing and contesting evidence from abroad: A defence perspective on cross-border evidence' (2011) Crim L.R. 1, pp. 40–57

Macan-Markar, M, 'Developing countries not immune from cybercrime—UN', Inter Press Service, posted 25 April 2005, available at <http://www.ipsnews.net/africa/internaasp?idnews=28430>.

Mann D and Sutton, M, 'NETCRIME: More change in the organization of thieving', pp 201–29, 38 *British Journal of Criminology*, 1998.

Martin, G., "The case of the hacked refrigerator – Could 'The Internet of Things' connect everything?", 5 February 2014, available at <http://alumni.berkeley.edu/california-magazine/just-in/2014-03-05/case-hacked-refrigerator-could-internet-things-connect>

McAfee, *Virtual Criminology Report: North American Study into Organised Crime and the Internet*, July 2005, available at <http://www.softmart.com/mcafee/docs/McAfee%20NA%20Virtual% 20Criminology%20Report.pdf>.

McGee, S., R. Sabett and A. Shah, "Adequate attribution: A framework for developing a national policy for private sector use of active defense", 8 J. Bus. & Tech. L. 1 (2013)

Mirfield, P, 'Regulation of Investigatory Powers Act 2000 (2): Evidential aspects' [2005] Crim LR 91.

Moitra, SD,

(a) 'Analysis and modelling of cybercrime: prospects and potential', *Max Planck Institute for Foreign and International Criminal Law*, available at: <https://www.mpicc.de/shared/data/pdf/fa-moitra03.pdf>.

(b) 'Developing policies for cybercrime: Some empirical issues', pp 435–64, *European Journal of Crime, Criminal Law and Criminal Justice*, vol 13, No 3, 2005.

Nikkel, B, 'Domain name forensics: A systematic approach to investigating an internet presence', *Digital Investigation* 1, 247–55, 2004.

Noam, E, 'Beyond liberalization II: The impending doom of common carriage', pp 435–52, *Telecommunications Policy*, vol 18, No 6, 1994.

Nykodym, N, Taylor, R, and Vilela, J, 'Criminal profiling and insider cyber crime', pp 408–14, *Computer Law and Security Report*, vol 21, No 5, 2005.

O'Brian Jr, W, 'Court scrutiny of expert evidence: Recent decisions highlight the tensions' 7 *E & P* 172, 2003.

O'Brien, M, 'Clear and present danger? Law and the regulation of the Internet', pp 151–64, *Information & Communications Technology Law*, vol 14, No 2, 2005.

O' Floinn and Ormerod, D,:

(a) 'Social networking sites, RIPA and criminal investigations', *Crim. L. R.* 2011, 10, 766-789

(b) 'Social Networking Material as Criminal Evidence', *Criminal Law Review*, 7 (2012), 486.

Olivenbaum, JM, '<CTRL><ALT><DEL>: Rethinking federal computer crime legislation', 27 *Seton Hall Law Review* 574, 1997.

Ormerod, D,
(a) 'Case Comment', [2000] Crim LR, May, 385–388.
(b) 'Improving the disclosure regime', pp 102–129, *International Journal of Evidence and Proof*, vol 7, no 2, 2003.
(c) 'Telephone intercepts and their admissibility', [2004] Crim LR 15.
(d) 'Entrapment: Restating principles and reviewing recent developments', paper delivered at CPS Conference, *Prosecuting Organised Crime*, 24 March 2006.

Paganini, P., 'Sinkholes: Legal and Technical Issues in the Fight against Botnets' (28 May 2014), available at <http://resources.infosecinstitute.com/sinkholes-legal-technical-issues-fight-botnets/>

Palfrey, T,
(a) 'Case Comments', [2000] Crim L.R, May, 385–388.
(b) 'Surveillance as a response to crime in cyberspace', pp 173–93, *Information and CommunicationsTechnology Law*, vol 9, No 3, 2000.
(c) 'Is fraud dishonest? Parallel proceedings and the role of dishonesty', pp 518–40, *The Journal of Criminal Law*, vol 64, pt 5, 2000.
(d) 'Cybercrimes and the fight against Hi-Tech criminality', paper delivered at a seminar organised by the European Institute of Public Administration, in Bucharest, 21–22 February 2005.

Philippsohn, S, 'Trends in cybercrime: An overview of current financial crimes on the Internet', 20 *Computers & Security*, pp 53–69, 2001.

Podgor, ES, 'International computer fraud: A paradigm for limiting national jurisdiction', 35 *UC Davis Law Review*, 267.

Poullet, Y, 'The fight against crime and/or the protection of privacy: A thorny debate!', pp 251–73, *International Review of Law Computers & Technology*, vol 18, No 2, 2004.

Quinn, K, 'Computer evidence in criminal proceedings: Farewell to the ill-fated s 69 of the Police and Criminal Evidence Act 1984', pp 174–187, *International Journal of Evidence and Proof*, vol 5, No 3, 2001.

Rauhofer, J, and Mac Sithigh, D, "The Data Retention Directive Never Existed", (2014) 11:1 SCRIPTed 118.

Redmayne, M, 'Disclosure and its discontents' [2004] Crim LR 441.

Reid, AS and Ryder, N, 'The case of Richard Tomlinson: The spy who emailed me', pp 61–78, *Information and Communications Technology Law*, vol 9, No 1, 2000.

Reidenberg, J,
(a) 'Lex Informatica: The formulation of information policy rules through technology', 76 *Texas Law Review*, 553, 1998.
(b) 'States and Internet enforcement', 1 *University of Ottawa Law and Technology Journal*, 1, 18, 2004.

Reitinger, PR,
(a) 'Compelled production of plaintext and keys', 171, *University of Chicago Legal Forum*, 1996.
(b) 'Encryption, anonymity and markets', in Thomas, D and Loader, B (eds), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, 2000.

Rowbottom, J, 'Obscenity laws and the Internet: Targeting the supply and demand', pp 97–109, [2006] *Criminal Law Review*.

Rowland, D, 'Data retention and the war against terrorism—A considered and proportionate response?', (3) *Journal of Information, Law and Technology (JILT)* 2004, available at <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/rowland/>.

Ryan, PS, 'War, peace or stalemate: Wargames, wardialing, wardriving and the emerging market for hacker ethics', *Virginia Journal of Law & Technology*, vol 9, No 7, Summer 2004.

Salgado, R, 'Legal issues', pp 225–52, in *Know your Enemy*, Addison-Wesley, 2004.

Samuelson, P, 'Legally speaking: Can hackers be sued for damages caused by computer viruses?, pp 666–9, *Communications of the ACM*, 32, 1989.

Sealey, P, 'Remote forensics', pp 261–65, *Digital Investigation* 1, 2004.

Seitz, N, 'Transborder search: A new perspective in law enforcement?', pp 23–50, *Yale Journal of Law and Technology*, Fall 2004–05.

Shytov, A, 'Indecency on the Internet and international law', pp 260–80, *International Journal of Law and Information Technology*, vol 13, No 2, 2005.

Sinrod, E and Reilly, W, 'Cyber-crimes: A practical approach to the application of Federal computer crime laws', pp 177–229, *Santa Clara Computer and High Technology Law Journal*, vol 16, May 2000.

Smith, G, 'An Electronic Pearl Harbor? Not likely', *Issues on Science and Technology*, 15, pp 68–73, Fall 1998.

Soghoian, C., 'Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era', *Journal on Telecommunications and High Technology Law*, 8(2) (2010), 359.

Sommer, P,

(a) 'Digital footprints: Assessing computer evidence', *Criminal Law Review*, Special Edition, December 1998.

(b) 'Evidence in Internet paedophilia cases', pp 176–84, *Computer and Telecommunications Law Review*, vol 8, No 7, 2002.

(c) 'Evidence from cyberspace: Downloads, logs and captures', pp 33–42, *Computer and Telecommunications Law Review*, vol 8, No 2, 2002.

(d) 'Intrusion detection systems as evidence', pp 67–76, *Computer and Telecommunications Law Review*, vol 8, No 3, 2002.

(e) 'Computer misuse prosecutions', pp 25–6, *Computers and Law*, vol 16, No 5, December/January 2006.

Spence, M and Endicott, T, 'Vagueness in the scope of copyright', pp 657–80, *Law Quarterly Review*, vol 121, No 4, 2005.

Spencer, JR, 'Codifying criminal procedure' [2006] Crim LR 279.

Steele, D, 'Eavesdropping on electromagnetic radiation emanating from video display units' (1989–90) 32 *Criminal Law Quarterly*, 253.

Sussmann, M, 'The critical challenges from international high-tech and computer-related crime at the millennium', 9 *Duke J of Comp & Int'l L* 451.

Tapper, CB, 'Criminality and copyright', pp 266–79, in Vaver, D, and Bently, L (eds), *Intellectual Property in the New Millennium*, Cambridge University Press, 2004.

Taylor, M, Holland, G, and Quayle, E, 'Typology of paedophile picture collections', 74 *Police Journal* 97, 2001.

Taylor, MJ, Haggerty, D, Gresty and Hegarty, R, "Digital evidence in cloud computing systems", pp. 304-308, *Computer Law and Security Review*, 26(3), 2010

Thomas, D, 'Criminality on the electronic frontier', pp 17–35, in Thomas, D and Loader, B (eds), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, 2000.

Turner, P, 'Digital provenance—interpretation, verification and corroboration', pp 45–9, *Digital Investigation* 2, 2005.

Urbas, G, 'Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement', *Journal of Internet Law*, 16(1) (2012), 7.

Vegh, S, 'Hackivists or cyberterrorists? The changing media discourse on hacking' 7(10) *First Monday*, at <http://firstmonday.org/issues/issue7_10/vegh/index.html>.

Walden, I,

(a) 'Computer crime', pp 295–29, Chapter 8 in *Computer Law*, 7th edition, Reed (ed), Oxford University Press, 2011.

(b) 'Crime and Security in Cyberspace', pp 51–68, in *Cambridge Review of International Affairs*, vol 18, No 1, April 2005.

(c) 'Harmonising computer crime laws in Europe', pp 321–36 in *European Journal of Crime, Criminal Law and Criminal Justice*, vol 12, No 4, 2004.

(d) 'Addressing the data problem', pp 18–31, *Information Security Technical Report*, vol 8, No 2, 2003.

(e) 'Honeypots: A sticky legal landscape' (with Anne Flanagan), pp 317–70, in *Rutgers Computer and Technology Law Journal*, vol 29, No 2, 2003.

Walden, I., and M. Wasik, 'The Internet: Access Denied Controlled!', pp. 377–387, [2011] *Crim. L.R.*, Issue 5.

Walker, C, 'Email interception and RIPA: the Court of Appeal rules on the "right to control" defence', pp 22–4, *Communications Law*, vol 11, No 1, 2006.

Wall, DS,

(a) 'Policing and the regulation of the Internet', pp 79–91, in Walker, C (ed), *Crime, Criminal Justice and the Internet* (special edition, *Criminal Law Review*), Sweet & Maxwell, London, 1998.

(b) 'Cybercrimes: New wine, no bottles?', in Davies, P, Francis, P, and Jupp, V (eds), *Invisible Crimes: Their Victims and their Regulation*, Macmillan, 1999.

(c) 'Policing the Internet: Maintaining order and law on the cyberbeat', Chapter 7, pp 154–75, in Walker, C and Wall, D (eds), *The Internet, Law and Society*, Longman, 2000.

(d) 'The Internet as a conduit for criminals', pp 77–98, in *The Criminal Justice System and the Internet*, Pattavina, A (ed), Thousand Oaks, 2005.

Wallace, RP, Lusthaus, A, and King, JH, 'Computer crimes', 42 *American Criminal Law Review* 223, 2005.

Warren, P, 'Smash and grab, the hi-tech way', *The Guardian*, 19 January 2006.

Wasik, M, 'Hacking, viruses and fraud', Chapter 12, pp 272–93, in Walker, C and Wall, D (eds), *The Internet, Law and Society*, Longman, 2000.

Wegener, H, 'Guidelines for national criminal codes on cybercrime', available at <http://www.itis-ev.de/infosecur>, 31 July, 2003.

White, M, 'Far right extremists on the Internet', pp 234–50, in Thomas, D and Loader, B (eds), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, 2000.

White, S, 'Harmonisation of criminal law under the first pillar', pp 81–92, 31 *European Law Review*, February 2006.

Wible, B, 'A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime', pp 1577–624, *Yale Law Journal*, vol 112, No 6, 2003.

Williams, K, 'Controlling Internet child pornography and protecting the child', pp 3–24, *Information & Communications Technology Law*, vol 12, No 1, 2003.

Williams, P, 'Organised crime and cybercrime: synergies, trends and responses', 2001, available from <http://www.crime-research.org>.

Wilson, W, 'The structure of criminal defences' [2005] Crim LR 108.

Wong Yang, D and Hoffstadt, B, 'Countering the cyber-crime threat' 43 *American Criminal Law Review* 201, 2006.

Yong, P., 'New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime', December 2011, available at <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042f0>.

Zhengchuan Xu, Qing Hu, and Chenghong Zhang: "Why computer talents become computer hackers", *Communications of the ACM*, April 2013, vol. 56, no. 4.

REPORTS, OFFICIAL DOCUMENTS

All Party Parliamentary Internet Group:

Report on 'Communications Data', January 2003.

Report on 'Revision of the Computer Misuse Act', June 2004.

Association of Chief Police Officers, 'Good Practice Guide for Computer Based Evidence' (3rd edn).

Association Internationale pour la Protection de la Propriété Intellectuelle (AIPPI) Summary Report, 'Criminal law sanctions with regard to the infringement of intellectual property rights' (Question 169), 2002. Available from <http://www.aippi.org>.

Attorney-General:

Guidance on Disclosure, April 2005.

Section 18 RIPA Prosecutors Intercept Guidelines England and Wales.

'guidelines for prosecutors on the use of the common law offence of conspiracy to defraud', available at <https://www.gov.uk/use-of-the-common-law-offence-of-conspiracy-to-defraud--6>

Cabinet Office, Performance and Innovation Unit Report, *Encryption and Law Enforcement*, May 1999.

Computer Security Institute and Federal Bureau of Investigation ('CSI/FBI Survey'), *Computer Crime and Security Survey*, annually since 1995, available from <http://www.goci.com>.

Council of Europe:

'Extraterritorial criminal jurisdiction', 1990.

Cybercrime Convention Committee paper, *Strengthening co-operation between law enforcement and the private sector—Examples of how the private sector has blocked child pornographic sites*, T-CY (2006) 04, 20 February 2006.

T-CY Guidance Note # 2, 'Provisions of the Budapest Convention covering botnets', T-CY (2013) 6E Rev

Electronic evidence guide (Ver. 1, March 2013)

T-CY Guidance Note # 5, 'DDOS attacks', T-CY (2013) 10E Rev

T-CY, Guidance Note # 3, *Transborder access to data (Article 32)*, 3 December 2014

Crown Prosecution Service

Code for Crown Prosecutors (2013)

Guidelines for prosecutors on assessing the public interest in cases involving the media, September 2012

Department of Trade and Industry:

Dealing with Computer Misuse, HMSO, 1992.

Consultation Document, *Building Confidence in Electronic Commerce* (URN 99/642), March 1999.

European Commission:.

Commission Communication to the Council and the European Parliament on 'Critical Infrastructure Protection in the fight against terrorism', COM(2004) 702 final, Brussels, 20 October 2004.

Commission Communication to the European Parliament and the Council on 'the implications of the Court's judgment of 13 September 2005' (Case C 176/03 *Commission v Council*), COM(2005) 583 final, Brussels, 23 November 2005.

Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final, 17112005.

Commission Communication, 'Consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures' COM(2009) 665 final, 2.12.2009.

Commission Communication, 'Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law', COM(2011) 573 final, 20.9.2011

Commission Communication, 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', COM(2012) 140 final, 28.3.2012

Commission Staff Working Document, *E-commerce Action Plan*, 2012-2015, Brussels, 23.4.2013

Europol:

Computer-related crime within the EU: Old crimes new tools; new crimes new tools (2002).

HM Government

A Strong Britain in an Age of Uncertainty: The National Security Strategy (Cm 7953), October 2010

Decision pursuant to Article 10 of Protocol 36 to The Treaty on the Functioning of the European Union, Cm 8671, July 2013

Serious and Organised Crime Strategy (Cm 8715), October 2013

Response to the House of Lords EU Committee Inquiry on the UK's 2014 opt-out decision (6 January 2014)

Home Affairs Committee Report No 126: 'Computer Pornography', HMSO, February 1994.

Home Office:

Consultation Paper, *Interception of Communications in the United Kingdom*, Cm 4368, June 1999.

Consultation Paper, *Accessing Communications Data: Respecting Privacy and Protection the Public from Crime*, 11 March 2003.

Discussion Paper, *Counter-Terrorism Powers: Reconciling Security and Liberty in an Open Society*, Cm 6147, February 2004.

Online Report 62/04, *The future of netcrime now: Part 1— threats and challenges.*

Online Report 63/04, *The future of netcrime now: Part 2— responses.*

Criminal Statistics: England and Wales 2003, Cm 6361, 2004.

Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside the United Kingdom (12th edn), March 2015

Consultation Paper, 'The initial transposition of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC', March 2007.

Investigation of Protected Electronic Information, 2007.

Intercept as Evidence, December 2009, Cm 7760

Surveillance Camera Code of Practice, June 2013

Circular, *Serious Crime Act 2015*, March 2015.

Counting Rules for Recorded Crime, available at https://www.gov.uk/government/publications/counting-rules-for-recorded-crime.

Cyber crime: A review of the evidence, Research Report 75, October 2013. Available at https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Covert Human Intelligence Sources: Code of Practice, December 2014

Covert Surveillance and Property Interference, December 2014.

Acquisition and Disclosure of Communications Data, March 2015.

Interception of Communications Code of Practice, January 2016.

Equipment Interference Code of Practice, January 2016.

Consultation Paper, *On the possession of extreme pornographic material,* August 2005.

Online Report 09/06, *Fraud and technology crimes: Findings for the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources.*

Consultation Paper, *Investigation of Protected Electronic Information*, June 2006.

Consultation Paper, *New Powers Against Organised and Financial Crime,* Cm 6875, HMSO, July 2006.

Consultation on the possession of extreme pornographic material: Summary of responses and next steps, August 2006.

Independent Reviewer of Terrorism Legislation, *A Question of Trust*, June 2015.

Information Assurance Advisory Council, *Digital Evidence, Digital Investigations and E-Disclosure*, 4th edition, November 2013.

Information Commissioner, *What Price Privacy? The unlawful trade in confidential personal information*, 10 May 2006.

Intellectual Property Office,

Report: *Penalty Fair? Study of criminal sanctions for copyright infringement available under the CDPA 1988*, 2015

A consultation on changes to the penalties for offences under sections 107(2A) and 198(1A) of the Copyright Designs and Patents Act (Penalties for Online Copyright Infringement, 18 July 2015

Intelligence and Security Committee report, *Privacy and Security: A modern and transparent legal framework*, HC 1075, March 2015

Interception of Communications Commissioner:

Report for 2002 (September 2003).

Report for 2003 (July 2004).

Law Commission:

Working Paper No 31, *The Mental Element in Crime*, HMSO, 1970.

Report No 55, *Report on Forgery and Counterfeit Currency*, HMSO, 1973.

Report No 91, *Report on the Territorial and Extraterritorial Extent of the Criminal Law*, Cm 75, HMSO, 1978.

Working Paper No 110, *Computer Misuse*, HMSO, 1988.

Report No 177, *A Criminal Code for England and Wales*, HMSO, 1989.

Report No 180, *Jurisdiction over Offences of Fraud and Dishonesty with a Foreign Element*, Cm 318, HMSO, 1989.

Report No 186, *Computer Misuse*, Cm 819, HMSO, 1989.

Report No 243, *Offences of Dishonesty: Money Transfers*, HMSO, 1996.

Consultation Paper No 150, *Legislating the Criminal Code: Misuse of Trade Secrets*, HMSO, 1997.

Consultation Paper No 155, *Legislating the Criminal Code: Fraud and Deception*, HMSO, 1999.

Report No 276, *Fraud*, Cm 5569, HMSO, 2002.

Report No 300, *Inchoate Liability for Assisting and Encouraging Crime*, Cm 6878, HMSO, July 2006.

Tenth Programme of Law Reform, 2008.

National Criminal Intelligence Service report, 'Project Trawler: Crime on the Information Highways' (1999), available at <http://www.cyber-rights.org>.

National Infrastructure Security Co-ordination Centre:

Briefing 08/2005, *Targeted Trojan Email Attacks*, 16 June 2005.

Briefing 11a/2005, *Botnets—The threat to the Critical National Infrastructure.*

OECD, 'Computer-Related Criminality: Analysis of Legal Policy in the OECD Area', Report DSTI-ICCP 8422 of 18 April 1986.

Office of Communications (Ofcom) (and formerly Oftel):

Guidelines for the Interconnection of Public Electronic Communication Networks, May 2003.

Research Document, 'Online protection: A survey of consumer, industry and regulatory mechanisms and systems', 21 June 2006.

Office of the President, *The National Strategy to Secure Cyberspace* 39 (Feb 2003), at <http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf>.

Oxford Internet Institute survey report, *The Internet in Britain*, May 2005: available from <http://www.oii.ox.ac.uk/>.

Privy Council Review of Intercept as Evidence, 30 January 2008, Cm 7324.

RAND Technical Report, Handbook of Legal Procedures of Computer and Network Misuse in EU Countries, 2006; available from <http://www.rand.org>.

Royal United Services Institute, Independent Surveillance Review, *A Democratic Licence to Operate*, July 2015

Sentencing Guidelines Council (formerly the Sentencing Panel):

'The Panel's Advice to the Court of Appeal on Offences Involving Child Pornography', August 2002.

'Sexual Offences Act 2003: Consultation Guideline', June 2006.

Serious and Organised Crime Agency, The United Kingdom Threat Assessment of Serious Organised Crime: 2006/7, 31 July 2006.

United Nations:

United Nations Manual on the Prevention and Control of Computer-related Crime, United Nations publication, Sales No E95IV5. Published in the *International Review of Criminal Policy*, Nos 43 and 44, 1996: available at <http://www.uncjin.org/Documents/EighthCongress.html#congress>. 'Measures to Combat Computer-related Crime', Workshop 6: Background Paper (A/CONF203/14), presented at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, April 2005.

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, draft, (February 2013)

US Department of Defense, Annual Report to Congress, *The Military Power of the People's Republic of China*, 20 July 2005.

US Department of Justice Report, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, July 2002 (available at <http://www.usdoj.gov/criminal/cybercrime>).

United States Sentencing Commission, *Guidelines Manual* (2014), available at <http://www.ussc.gov/guidelines-manual/2014/2014-ussc-guidelines-manual>.

World Federation of Scientists, Permanent Monitoring Panel on Information Security, *Towards a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, August 2003.