THE UNIVERSITY of EDINBURGH

Do organisations in the UK have a legal right to implement Data Loss Prevention technology with respect to employee's personal devices?

Joel Greenwell

Submitted in accordance with the requirements for the degree of
Master of Laws

The University of Edinburgh

August 2013

The candidate confirms that the work submitted is his/her own and that appropriate credit has been given where reference has been made to the work of others.

Contents

Introduction

There are two technology paradigms that have become predominant within the past few years, which are converging upon each other much like two huge cargo ships, "Data Loss Prevention" (DLP) and "Bring your own Device" (BYOD). Understanding the legal implications of such a convergence is important to ensure organisations don't become exposed themselves to potential legal difficulties.

Starting with a brief introduction to DLP and BYOD, explaining their history and what they are, this dissertation will continue with a more detailed analysis on why organisations choose to implement these technologies.

Based upon this background an overview will be presented with respect to applicable UK and international legislation and the use of DLP and BYOD technologies when combined within a single environment. Will these two technologies comfortably reside together when balancing the rights of the employee, against those of the employer? Let's proceed to find out.

What is Data Loss Prevention (DLP)?

Rich Mogull[1] of Securosis[2] succinctly explains DLP as
"Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis."[3]

Data at rest is data stored within digital storage mediums such as computer hard drives, storage on networks, anywhere where data can be retained and accessed later for use. Data in motion is the transfer of data between storage mediums, such as copying files via network connections, or using locally connected storage devices. Data in use is where the data is being accessed by

[1] Founder of Securosis and former Research Vice President at Gartner on the security team, http://searchcloudsecurity.techtarget.com/contributor/Rich-Mogull
[2] https://securosis.com/
[3] Understanding and Selecting a Data Loss Prevention Solution, Rich Mogull, https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf
Published:- 04/12/2007, Checked online:- 30/06/2013

systems or applications for the purposes of further processing and generation of results from such processing, which can include changing the source data.

There are several products on the market that provide DLP solutions, with those considered leaders in this technology independently compared and contrasted by Gartner, based upon the "Magic Quadrant"[4] model.

Why do Organisations implement DLP solutions?

When organisations commit to expenditure and resources, especially for large projects, there has to be a clear justification in order to establish an understanding on the objectives and purpose of the project. DLP can be considered as "risk mitigation" implementation rather than "revenue generation" and much like insurance company actuaries, organisations need to balance between the financial costs of such projects against the possible consequences of not investing in a DLP solution. The following will explain why companies invest in DLP solutions and what risks are mitigated as a result.

Protecting Reputation

Consumer confidence in a companies' product or service can make or break a business. The phrase "Doing a Ratner"[5], illustrates how loss of reputation can have devastating consequences, which in the case of Ratners devalued the business by £500 million extremely quickly. The finance industry can consider reputation as its "life blood", and a loss of reputation can lead to funding problems, halting inter-banking transactions and a "run on the bank" as in the case of Northern Rock crisis in 2007[6]. Loss of reputation within the financial industry is "infectious", especially from the perspective of depositors who wrongly associate separate financial institutions governed by the same regulator to be a risk for their deposits, and consequently

[4] Magic Quadrant for Content-Aware Data Loss Prevention, Eric Ouellet, http://www.computerlinks.de/FMS/22876.magic_quadrant_for_content_aware_data_loss_prevent.pdf, Published:- 03/01/2013, Checked online:- 30/06/2013
[5] Telegraph Article, 'Doing a Ratner' and other famous gaffes, http://www.telegraph.co.uk/news/uknews/1573380/Doing-a-Ratner-and-other-famous-gaffes.html, Published 22/12/2007, Checked online:- 07/07/13
[6] The failure of Northern Rock: A Multi-dimensional Case Study ISBN-13: 978-3-902109-46-0, Page 19 http://www.suerf.org/download/studies/study20091.pdf, Published:- 2009, Checked online:- 07/07/13

withdraw all their investments from the same banking sector, with potentially dire consequences[7].

Having established that loss of reputation can have a severe impact, especially in the financial sector, how does this relate to DLP? A case study of 5 private Dutch Banks[8] showed that the respondents surveyed were most concerned about reputational loss[9] in the event of an IT security incident that breached confidentiality. A report by Advisen[10] titled "The Reputational Risk of a Data Breach"[11] includes a reference to a survey of 3,000 consumers where 15% would immediately leave the organisation and a further 39% would consider leaving the organisation if advised of a data breach.

Organisations realise that reputational damage has a severe impact to the business, and must endeavour where wherever possible to reduce the risk of a sullied reputation from events such as data breaches. Investment in DLP technology is part of the arsenal of technologies that organisations can deploy with the objective of reputation protection.

Preventing Insider Data Theft – Rise of the Frienemy[12]

When considering data theft, the concept of "us" and "them", where "us" are those within the organisation, and "them" is everyone else; it is easier to understand the lines of security demarcation. However when the "them" includes parties within the organisation (employees, sub-contractors, suppliers etc) who may not have the organisations' best interests in mind, this delimitation no longer exists. In the interests of workable relationships, it would be unreasonable

[7] Reputational Contagion and Optimal Regulatory Forbearance, http://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1196.pdf, Published:- May 2010, Checked online:- 06/07/2013

[8] Exploring ways to Model Reputational Loss, Cas de Bie, http://www.jbisa.nl/download/?id=8762035, Checked online: - 06/07/2013

[9] Ibid Page 63

[10] http://www.advisen.com

[11] The Reputational Risk of a Data Breach, Virginia Citrano and David Bradford http://corner.advisen.com/pdf_files/Reputational_Risk_Data_Breach_2012NAS.pdf, Published:- 29/09/2012, Checked online:- 06/07/2013

[12] A portmanteau of "friend" and "enemy" first coined by Walter Winchell in a article titled "Howz about calling the Russians our Frienemies?" published in an article published in the Nevada State Journal on the May 19, 1953. Describes those who pose as your friend, but whose intentions are not in your best interests.

to consider all parties with suspicion, and this is where DLP technologies can provide an unbiased approach in preventing data being misappropriated.

Research performed by Ponemon Institute LLC[13] (Ponemon), showed that negligent employees and criminal insiders were the highest cause of data breaches across eight countries[14]. In the UK the Credit Industry Fraud Avoidance System (CIFAS)[15], published a report in April 2013[16] that showed there has been an increase of employees unlawfully obtaining personal and commercial data between 2011 and 2012[17], with the greatest proportion of offences being committed within the finance sector[18]. The report also indicated that the uptake of "Bring your own device" (BYOD) to allow employees to use their personal device for work purposes has raised concerns that the opportunity for insider data theft has increased considerably. Note the statistics gathered by CIFAS must satisfy a standard of proof[19], therefore unreported instances could be a lot higher, given the reputational risk when disclosing data breaches.

ID Analytics[20] published a whitepaper[21] included two case studies explaining the methods employed by employees to deliberately steal data from their employer to be used for fraudulent purposes. Understanding why individuals risk undertaking such illegal activity that could lead to severe penalties, is important to establish the most likely "modus operandi" in ensuring the most effective methods are used when implementing DLP technologies.

[13] 2011 Cost of Data Breach Study: Global, Ponemon Institute LLC
http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf
Published:- 17/07/2013, Checked online:- 06/07/2013
[14] Ibid page 6
[15] http://www.cifas.org.uk/
[16] Staff Fraud Scape. Depicting the UK's fraud landscape, CIFAS
https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Staff_Fraudscape_CIFAS_webversion.pdf
Published:- 03/04/2013, Checked online:- 06/07/2013
[17] Ibid page 6
[18] Ibid page 7
[19] Ibid page 3
[20] http://www.idanalytics.com/
[21] Analysis of Internal Data Theft, ID Analytics Inc,
http://www.idanalytics.com/assets/whitepaper/IDAnalyticsInternalDataTheftWhitepaper071808.pdf, Published 28/07/2008, Checked online:- 07/07/1013

Carnegie Mellon University[22] published research that investigated 48 cases of Intellectual Property (IP) theft in the USA, and proposed two models to explain what drove individuals to steal data. The "The Entitled Independent Model"[23], where individuals felt that given they developed or partially developed the IP; it was their right to take the information with them, and the "The Ambitious Leader Model"[24]where insiders were motivated to steal data under the direction of someone else, where these leaders would typically recruit or bring colleagues with them to their next placement. Both models are very similar, with the sense of entitlement being the largest factor, the key difference being ambitious leaders had more time and resource and an overall plan with respect to the theft and use of stolen IP.

Further research on the employee attitude to corporate data was conducted by Ponemo[25], which included a survey on software developers within 6 different countries and asking if they considered it acceptable to reuse source code created for previous employers. An average of 44% of respondents considered this practice as their right to do so, supporting the Carnegie Mellon University research. The survey also showed that 41% of employees downloaded company confidential information to personal devices without asking for permission, with 40% stating they would use such information in their new jobs. Organisations need to be prepared to meet such attempts of IP theft with appropriate measures such as DLP, especially if there are any indications that employees are about to "jump ship".

The uptake of BYOD within organisations leading to a greater threat to the theft of data is identified within another report released by Ponemon titled "The Risk of Insider Fraud" second annual study[26]. This report indicated that insider fraud is getting worse and 44% of those interviewed strongly agreed that BYOD significantly introduced more security risks[27].

---

[22] "A Preliminary Model of Insider Theft of Intellectual Property" (2011). Software Engineering Institute, Paper 726. Moore, Andrew P.; Cappelli, Dawn; Caron, Thomas C.; Shaw, Eric D.; Spooner, Derrick; and Trzeciak, Randall F., http://repository.cmu.edu/sei/726,
Published:- 06/01/2011, Checked online:- 07/07/2013

[23] Ibid page 6

[24] Ibid page 10

[25] What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk, Symantec Corporation https://www4.symantec.com/mktginfo/whitepaper/WP_WhatsYoursIsMine-HowEmployeesarePuttingYourIntellectualPropertyatRisk_dai211501_cta69167.pdf
Published:- 01/02/2013, Checked online:- 07/07/2013

[26] The Risk Of Insider Fraud, Second Annual Study, Ponemon Institute LLC

From a UK perspective OnePoll[28] conducted a survey[29] on the behalf of LogRhythm[30], interviewing 2,000 employees, where 23% of those interviewed admitting taking confidential information from their employer, typically while still working for the current employer and after handing in their notice, with the intent of using this data in their next job. It is important to understanding that insider data theft is a very real threat for organisations, especially when digital assets can be taken with apparent ease and minimal risk to the perpetrators, and hence there is a very real need for DLP technology to secure these digital assets.

Legal Liabilities

Organisations within the United Kingdom are required to adhere to multiple pieces of legislation with respect to controlling information, especially regarding data held within Information and Communications Technology (ICT) infrastructure. Identifying the legal liabilities organisations have, subject to both UK and international legislation, and the possible consequences of not meeting these legal statutes is important to understand. Based upon sound legal reasons and understanding of their background, DLP technologies can be employed to assist organisations meet these legal obligations.

Data Protection Legislation

Different legal and regulatory obligations are applicable depending on the nature of business being conducted by the organisation, but all organisations are required to adhere to the Data Protection Act 1998 (DPA 1998)[31] when processing data that is considered to be personal[32].

---

http://www.unfaircompetitiontradesecretscounsel.com/PonemonInstituteTheRiskOfInsiderFraud.pdf Published:- 02/2013, Checked online:- 06/07/2013

[27] Ibid page 8

[28] http://www.onepoll.com/

[29] UK Insider Threat – consumer, OnePoll Survey, Marshall Andria http://logrhythm.com/Portals/0/resources/LogRhythm_survey_results_4.2013_employees.pdf, Published:- 10/05/2013, Checked online:- 07/07/2013

[30] http://logrhythm.com/

[31] Data Protection Act 1998, 1998 CHAPTER 29, http://www.legislation.gov.uk/ukpga/1998/29/contents, Enacted 16/071998, Checked online: -11/08/2013

[32] Data Protection Act 1998, What is personal data? – A quick reference guide, http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf, Published: -18/04/2008, Checked online:- 11/08/2013

The Act has been amended in lieu of several high-profile data security breaches, which include: -

- The loss of two CD's containing child benefit data, which included personal information pertaining to 7.5 million individuals[33].
- Theft of a Ministry of Defence laptop which held personal information regarding approximately 600,000 applicants wishing to enlist within the military[34].

Such was the seriousness of these and other incidents, that a Justice Committee was appointed to look into the matter of data privacy[35], making several recommendations with respect to changes in the law.

The amendments to the DPA 1998 include empowering the Information Commissioner's Office (ICO)[36] to levee a penalty[37] as inserted by section 144 of the Criminal Justice and Immigration Act 2008[38]. The authority for the ICO to legally impose a fine was conferred on the 6th April 2010 via The Data Protection (Monetary Penalties) Order 2010[39]. Legislation doe not yet allow custodial sentences to be sentenced for breach of section 55[40] of the DPA, however the Joint

[33] Independent police complaints commission, IPCC, independent report into loss of data relating to Child Benefit, Emma Bryan, http://www.ipcc.gov.uk/Documents/investigation_commissioner_reports/final_hmrc_report_25062008.pdf, Published: -24/06/2008, Checked online:- 11/08/2013

[34] House of Commons, Hansard Debates., 21 January 2008, c1225 http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080121/debtext/80121-0006.htm#0801215000512, Checked online:- 11/08/2013

[35] House of Commons, Select Committee on Justice, First Report, Problems with data protection http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/15402.htm, Published: - 17/12/2007, Checked online:- 11/08/2013

[36] http://www.ico.gov.uk

[37] Information Commissioner's guidance about the issue of monetary penalties prepared and issued under Section 55C (1) of the Data Protection Act 1998, ISBN: 9780108511240, http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.ashx, Published 2012, Checked online:- 11/08/2013

[38] Criminal Justice and Immigration Act 2008, 2008 c. 4 Part 11 Penalties for serious contraventions of data protection principles, Section 144, http://www.legislation.gov.uk/ukpga/2008/4/section/144/prospective#section-144-1, Enacted: - 8th May 2008, Checked online:- 11/08/2013

[39] The Data Protection (Monetary Penalties) Order 2010, Statutory Instruments, 2010 No. 910 http://www.legislation.gov.uk/uksi/2010/910/introduction/made, Came into force:- 06/04/2010, Checked online:- 11/08/13

[40] Data Protection Act 1998, 1998 c. 29 Part VI Unlawful obtaining etc. of personal data Section 55, http://www.legislation.gov.uk/ukpga/1998/29/section/55, Enacted 16/071998, Checked online: -11/08/2013

Committee on the Draft Communications Data Bill[41], Home Affairs Committee[42], House of Commons Justice Committee[43], the Leveson Inquiry[44] and Stephan Shakespeare's independent review of Public Sector Information[45] all recommend that the government commences sections 77 and 78 of the Criminal Justice and Immigration Act 2008 to allow for custodial sentences for breach of section 55[46]. The government response to these recommendations[47] is to refer to the Regulation of Investigatory Powers Act 2000[48] and the Computer Misuse Act 1990[49], as appropriate legislation, but omits commentary with respect to data breaches and commitment to custodial offences.

41

Draft Communications Data Bill - Draft Communications Data Bill Joint, Conclusion, and summary of recommendations, Section 316, http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7911.htm, Published: - 11/12/ 2012, Checked online: -11/08/2013

42 Ibid

43 The functions, powers and resources of the Information Commissioner, Ninth Report of Session 2012–13, House of Commons Justice Committee, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/962/962.pdf, Published:- 12/03/2013, Checked online: 21/07/13,

44 An Inquiry Into The Culture, Practices And Ethics Of The Press Executive Summary, The Right Honourable Lord Justice Leveson, http://www.official-documents.gov.uk/document/hc1213/hc07/0779/0779.pdf, Published:- 11/2012, Checked online:- 21/07/2013

45 Shakespeare review of public sector information, Department for Business, Innovation & Skills, https://www.gov.uk/government/publications/shakespeare-review-of-public-sector-information, Published:- 15/05/2013, Checked Online:- 21/07/2013

46 The functions, powers and resources of the Information Commissioner, Ninth Report of Session 2012–13, House of Commons Justice Committee, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/962/962.pdf, Published:- 12/03/2013, Checked online:- 21/07/13

47 The Government Response to Shakespeare Review of Public Sector Information, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207600/Government_Response_to_Shakespeare_Review_of_Public_Sector_Information.pdf, Published:- June 2013, Checked online:-20/07/2013

48 Regulation of Investigatory Powers Act 2000, 2000 Chapter 23, http://www.legislation.gov.uk/ukpga/2000/23/contents, Enacted:- 28/07/2000, Checked online:- 11/08/2013

49 Computer Misuse Act 1990, 1990 Chapter 18, http://www.legislation.gov.uk/ukpga/1990/18/contents, Enacted:- 29/06/1990, Checked online:- 11/08/2013

Another outcome of the high-profile data security incidents was that the ICO commissioned a report[50] that introduced the term "Privacy Enhancing Technologies" (PETs) of which Data Loss Prevention (DLP)[51] facilitates part of the "Privacy by Design"[52] paradigm introduced within this report.

The implementation of DLP technology has been recognised by the ICO as suitable with respect to addressing data breaches[53], as per the incident of Co-Operative Life Planning Ltd[54], where information regarding 82,000 individuals was inadvertently published on the internet.

Under The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)[55], further amended by the 2011 regulations[56], the ICO is empowered to impose fines (maximum £500,000[57]) with respect to breaches of data privacy, within the domain of electronic communication.

---

[50] Privacy by design, Information Commissioner's Office, http://www.ico.org.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf, Published:- 11/2008, Checked online:- 11/08/2013

[51] Centre for the Protection of National Infrastructure, Critical control 17: Data loss prevention, http://www.cpni.gov.uk/advice/cyber/Critical-controls/in-depth/critical-control17/, Checked online:- 11/08/2013

[52] Privacy by design, Information Commissioner's Office, http://www.ico.org.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf, Published:- 11/2008, Checked online:- 11/08/2013

[53] ICO, Case Reference Number: ENF0379519, Undertaking by Co-operative Life Planning Ltd, http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/co-op_life_planning_undertaking.ashx, Checked online:- 11/08/2013

[54] ICO Press Release, Co-operative Life Planning commits to take action after thousands of customers' details were made available online http://www.ico.org.uk/~/media/documents/pressreleases/2011/coop_news_release_20110526.ashx, Published:- 26/05/2008, Checked online:- 11/08/2013

[55] The Privacy and Electronic Communications (EC Directive) Regulations 2003, Statutory Instruments, 2003 No. 2426, http://www.legislation.gov.uk/uksi/2003/2426/contents/made, Came into force:- 11/12/2010, Checked online:- 11/08/13

[56] The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, Statutory Instruments 2011 No. 1208, Electronic Communications http://www.legislation.gov.uk/uksi/2011/1208/contents/made Came into Force:- 20/05/2011, Checked online:- 11/08/2013

[57] Enforcing the revised Privacy and Electronic Communications Regulations (PECR), ICO http://www.ico.org.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/enforcing_the_revised_privacy_and_electronic_communication_regulations_v1.pdf Published:- 25/05/2011, Checked online:- 11/08/2013

Since the PECR came into force, the ICO has prosecuted and issued fines with respect to an organisation known as Tetrus Telecoms[58], which breached regulations 22 and 23 of the PECR. Two individuals were identified as being the owners and responsible for these breaches and were fined £300,000[59] and £140,000[60] respectively.

The basis upon which the PECR has been implemented within the UK is in direct response to the European Union Citizens Rights Directive[61] (Directive 2009/136/EC[62]). This directive of the European Parliament amends the following EU Directives and Regulation: -

- Directive 2002/22/EC[63] on universal service and users' rights relating to electronic communications networks and services
- Directive 2002/58/EC[64] concerning the processing of personal data and the protection of privacy in the electronic communications sector
- Regulation (EC) No 2006/2004[65] on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[58] Spam texters fined nearly half a million pounds as ICO cracks down on illegal marketing industry, ICO Press Release
http://www.ico.org.uk/news/latest_news/2012/spam-texters-fined-nearly-half-a-million-pounds-28112012
Published:- 28/12/2012, Checked online:- 11/08/2013
[59] ICO Monetary Penalty Notice [PECR], Mr Christopher Anthony Niebel trading as Tetrus Telecoms
http://www.ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Notices/tetrus_niebel_monetary_penalty_notice.ashx
Published:- 26/11/2012, Checked online:- 11/08/2013
[60] ICO Monetary Penalty Notice [PECR], Mr Gary John Peter McHeish trading as Tetrus Telecoms
http://www.ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Notices/tetrus_mcneish_monetary_penalty_notice.ashx,
Published:- 26/11/2012, Checked online:- 11/08/2013
[61] Explanatory Memorandum to The Privacy And Electronic Communications (EC Directive) (Amendment) Regulations 2011, 2011 No. 1208 http://www.legislation.gov.uk/uksi/2011/1208/pdfs/uksiem_20111208_en.pdf
Published:- 05/05/2011, Checked online:- 11/08/2013
[62] EU Directive 2009/136/EC of the European Parliament and of the Council, Official Journal of the European Union, L 337/11
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF
Published:- 18/12/2009, Checked online:- 11/08/2013
[63] EC Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0051:EN:PDF
Published:- 24/04/2002, Checked online:- 12/08/2013
[64] EC Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF
Published:- 31/07/2002, Checked online:- 12/08/2013

The European Commission proposed a reform of the data protection directive, releasing a press announcement on the 25/0/2012[66]. The primary objectives of the reform[67] is to establish a framework across all 27 member states for data protection and a directive relating to criminal offences associated with the breach of data privacy.

Article 30 sections 1 and 2[68] specify that the data controller and also the data processor must implement suitable technology to prevent any transfer of data that may contravene the proposed reform, whether accidental or not.

Article 31 requires organisations to report an incident of personal data breach within 24 hours to the appropriate supervisory authority[69], or provide an explanation if a notification took longer than 24 hours to be raised.

Article 79 provides the provision by which supervisory authorities may impose a fine up to €1 million (Euros) or 2%[70] of global turnover in the event an organisation breaches the regulations.

A report commissioned by the ICO[71], analysed the possible ramifications of the proposed reforms with regards to businesses within the UK. The report indicated that many organisations don't fully understand the implications of the proposed changes, both in relation to legal aspects,

---

[65] Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:364:0001:0001:EN:PDF
Published:- 09/12/2004, Checked online:- 12/08/2013

[66] Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, Reference: IP/12/46
http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en
Published:- 25/01/2012, Checked online:- 11/08/2013

[67] Explanatory Memorandum for the proposed new legal framework General Data Protection Regulation
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
Published:- 25/01/2012, Checked online:- 11/08/2013

[68] Ibid page 60

[69] Ibid page 60

[70] Ibid page 93

[71] Implications of the European Commission's proposal for a general data protection regulation for business, London Economics
http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Research_and_reports/implications-european-commissions-proposal-general-data-protection-regulation-for-business.ashx
Published:- 14/05/2012, Checked online:- 11/08/2013

costs and benefits. As a result the ICO has made a commitment to provide clear guidance for organisations, and raising awareness of such guidance[72].

Such comprehensive reforms has meant the process by which the proposed changes come into force has lead to much debate and negotiations between representatives of member states[73] and with apparently 4000 amendments having being submitted[74] including representations from business interests. Currently the reforms are with the Committee on Civil Liberties, Justice and Home Affairs (LIBE), where the appointed rapporteur (Jan Philipp Albrecht[75]) has released several amendments to the reform[76], such as extended the breach notification period from 24 to 72 hours and adding the provision for including procedures to ensure the security of personal data is preserved.

However the proposed amendments are not without controversy, leading to a minor "spat"[77] between Sarah Ludford[78] (Liberals and Democrat MEP and representing Alliance of Liberals and Democrats for Europe in the European Parliament (ALDE)[79]) and Jan Philipp Albrecht.

The European Data Protection Supervisor has also submitted commentary with regards to proposed amendments[80], which includes support for greater onus regarding accountability and

---

[72] Ibid page 11 (XI)
[73] COD - Ordinary legislative procedure (ex-codecision procedure) 2012/0011(COD)
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en#tab-0
Last Updated: - 08/03/2013, Checked online:- 11/08/2013
[74] EU to ease new data rules, Claire Davenport of Reuters
http://www.reuters.com/article/2013/06/06/eu-privacy-idUSL5N0EI2Q720130606
Published:- 06/06/2013, Checked online:- 11/08/2013
[75] Profile of Jan Philipp Albrecht, Group of the Greens/European Free Alliance
http://www.europarl.europa.eu/meps/en/96736/JAN+PHILIPP_ALBRECHT_home.html
Last Updated:- 12/07/2013, Checked online:- 11/08/2013
[76] Draft Report on General Data Protection Regulation, Jan Philipp Albrecht
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/924/924343/924343en.pdf
Published:- 16/01/2013, Checked online:- 11/08/2013
[77] EU Data Protection, dialogue on draft Regulation, Sarah Ludford Liberal Democrat MEP
http://www.sarahludfordmep.org.uk/node/2238
Published:- 29/05/2013, Checked online:- 11/08/2013
[78] Sarah Ludford Liberal Democrat MEP official website
http://www.sarahludfordmep.org.uk/
Checked online:- 11/08/2013
[79] Alliance of Liberals and Democrats for Europe in the European Parliament official website
http://www.alde.eu/
Checked online:- 11/08/2013

"lighten up"[81]on the requirements for notifications and bureaucracy, while raising concerns that notifying supervisory authorities for risky processing should remain[82].

It has been recognised that the duration concerning the review and discussion of the proposed EU data protection reform has certainly been longer than originally anticipated. The recent disclosure concerning of the NSA[83]' internet surveillance program "Prism"[84], has acted as a catalyst for expediting the process, prompting Viviane Reding (Vice-President of the European Commission, EU Justice Commissioner) to include within a speech[85], commentary that the proposed reforms should be enacted sooner than later. Viviane also makes reference to Chancellor Merkel's commitment for the new regulation, asking other member states to follow Germany's lead with a view to finalising the reform in May 2014, with the expectation it comes into effect for 2016.

Thus those organisations that understand the implications of the reform to the data protection directive will realise that implementing DLP technologies is pertinent within the next 2-3 years.

While the saga of the EU data protection reform proceeds (slowly), organisations that provide publicly available electronic communications services[86] such as internet service providers (ISPs) and telecommunication operators will be expected from the 25th of August 2013 to adhere to new EU regulations concerning breach notifications.

---

[80] Additional EDPS comments on the Data Protection Reform Package, European Data Protection Supervisor
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf
Published:- 15/03/2013, Checked online:- 11/08/2013
[81] Ibid
[82] Ibid
[83] United States National Security Agency, official website
http://www.nsa.gov/
Checked online:- 11/08/2013
[84] BBC News, Q&A: NSA's Prism internet surveillance scheme, Leo Kelion
http://www.bbc.co.uk/news/technology-23051248
Published:- 01/07/2013, Checked online:- 11/08/2013
[85] Women and the Web – Why Data Protection and Diversity belong together, Viviane Reding
http://europa.eu/rapid/press-release_SPEECH-13-637_en.htm
Published:- 15/07/2013, Checked online:- 11/08/2013
[86] ICO, The Guide to Privacy and electronic communications, section on Security of Services, Covell J
http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/security_of_services
Published:- 08/09/2011, Checked online:- 11/08/2013

The European Commission regulation No 611/2013 with respect to breach notifications[87], expects providers to notify competent nation authorities (which in the case of the UK would be the ICO), within 24 hours from detecting a data breach[88]. The regulation does have the provision for an extension of 3 days from the initial notification to gather all the required information to be provided to the competent authority[89], after which the provider will have to provide suitable justification on why the requested information could not be obtained within a 3 day period.

The regulation covers the specifics with regards to safeguarding leaked data via technical measures such as encryption[90] and by implementing Data Loss Prevention technologies, organisations are better placed to meet the requisite notification periods.

The wording of EU regulation No 611/2013 sets the tone for the possibility of this regulation being extended beyond organisations providing publicly available electronic communications services. Article 6 of this regulation requires a three year review to assess its effectiveness[91] and the question of extended the reach of this regulation to all organisations that hold personal data will no doubt be asked, especially if the proposed General Data Protection Regulations[92] have not been passed into law.

[87] Commission Regulation (EU) No 611/2013, on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications,
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
Published:- 24/06/2013, Checked online:- 11/08/2013
[88] Ibid Article 2, paragraph 2
[89] Ibid Article 2 paragraph 3
[90] Ibid Article 4 technological protection measures
[91] Commission Regulation (EU) No 611/2013, on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications,
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF,
Published:- 24/06/2013, Checked online:- 21/07/2013
[92] European Commission, Explanatory Memorandum for the proposed new legal framework General Data Protection Regulation
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
Published:- 25/01/2012, Checked online:- 11/08/2013

The European Commission has published a proposal for a Directive for Network and Information Security along with a cyber security strategy[93]including requirements concerning breach notifications.

The ICO consultation response to the EU Proposal[94] is mainly supportive, especially with regards to the legal requirement regarding the notification period. Interestingly the ICO pointed out that the notification requirement would address any delay that organisations may have considered in the past, as commercial confidence would be applied during the notification process.

The ICO did raise concerns about what data should be included within the notification, in that it should be kept to the absolute minimum, and the sharing of breach notifications via an international framework is questionable regarding benefits to be gained from sharing such information.

Therefore it is unlikely that breach notifications within the UK will require providers to disclose the details of individuals whose information has been leaked. Organisations would be expected to provide more of a synopsis regarding the scale of the breach, number of individuals impacted and what measures the provider is taking to inform those potentially impacted by the breach, and what has been done to mitigate the consequence of the breach.

Effective DLP measures include automated notification methods, indicating when attempted and successful data breaches (either mistakenly or deliberately) were detected and by whom. Organisations that have implemented DLP technologies will be better placed to meet existing and proposed pieces legislation, acts and regulations.

---

[93] EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive
http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
Published:- 07/02/2013, Checked online:- 12/08/2013

[94] Proposal for an EU Directive on Network and Information Security– ICO consultation response,
http://www.ico.org.uk/about_us/consultations/~/media/documents/consultation_responses/response-to-eu-directive-on-network-and-information-security-call-for-evidence-responses-to-consultations-and-inquiries.pdf,
Published:- 04/07/2013, Checked online:- 21/07/2013

Pharmaceutical Industry legal liabilities

When it comes to data processing via ICT systems, the pharmaceutical industry can be considered one of the largest and most diverse with respect to data collection, processing and analytics. Understanding legislation and regulations that applies to pharmaceutical industries operating in the UK with respect to computer data is a challenge, as there are both national and EU facets to be understood.

The pharmaceutical industry within the UK is regulated predominantly under Human Medicines Regulations 2012[95] (the 2012 Regulations), and some articles of the Medicines Act 1968[96] (the 1968 Act). It is the responsibility of the Medicines and Healthcare products Regulatory Agency (MHRA), to ensure all medicines and medical devices meet the minimum requirements with respect to safety and effectiveness. The MHRA is responsible for issuing licences as per Part II of the 1968 Act[97], and Part 1 Regulation 6 of the 2012 Regulations[98].

There are several types of licences that are issued and renewed by the MHRA[99], and revocation of a licence for failure to comply with GMP guidelines and requirements of the legislation can lead to those licences being revoked[100], and possibly penalties which include unlimited fines and/or a maximum 2 year prison sentence[101].

---

[95] The Human Medicines Regulations 2012, Statutory Instruments 2012 No. 1916, Medicines
http://www.legislation.gov.uk/uksi/2012/1916/contents/made
Came into force:- 14/08/2012, Checked online:- 11/08/2013

[96] Medicines Act 1968, 1968 CHAPTER 67
http://www.legislation.gov.uk/ukpga/1968/67
Enacted 25/10/1968, Checked online:- 11/08/2013

[97] Ibid Part II, Licences and Certificates Relating to Medicinal Products

[98] The Human Medicines Regulations 2012, PART 1 The licensing authority and the Ministers, Regulation 6,
http://www.legislation.gov.uk/uksi/2012/1916/regulation/6/made
Came into force:- 14/08/2012, Checked online:- 11/08/2013

[99] MHRA, Manufacturer's and wholesale dealer's licences,
http://www.mhra.gov.uk/Howweregulate/Medicines/Licensingofmedicines/Manufacturersandwholesaledealerslicences/index.htm
Last Updated 06/08/2013, Checked online:- 11/08/2013

[100] MHRA, List of Terminated, Revoked and Cancelled Manufacturing and Wholesale Dealer Licences 2010 – 2013, Alaka H
http://www.mhra.gov.uk/home/groups/is-lic/documents/publication/con062556.pdf
Last Updated 06/08/2013, Checked online:- 11/08/2013

[101] MHRA, Review of EU medicines legislation - proposals for implementation,
http://www.mhra.gov.uk/home/groups/comms-ic/documents/websiteresources/con007679.pdf
Published:- 21/03/2005, Checked online:- 11/08/2013

The MHRA Good Manufacturing (GMP) Inspectorate assesses pharmaceutical organisations with regards to Medicines Regulations 2012, which mostly implements EU legislation. The primary EU legislation is the EU Directive 2001/83/EC[102] relating to medicinal products for human use, which is further amended by EU Directive 2011/62/EU[103] relating to preventing falsified medical products entering into the supply chain. The EU Directive 2003/94/EC[104] sets out good practice regarding the manufacture of medical products for human use, which is obligatory as per Article 46 of the 2001 Directive.

When organisations are inspected by the MHRA GMP Inspectorate regarding licencing for manufacturer or distribution of medical products, the standards by which organisations are assessed are referenced within EU Directive 2003/94/EC, the detail of which is further explained within EudraLex - Volume 4 GMP guidelines[105].

The EudraLex publications cover all aspects of GMP guidelines, including the topic of Computerised Systems[106]. Section 12.4 of Annex 11 specifically covers the topic of management systems for documents and data, where the implementation of DLP technologies will be appropriate to meet such requirements.

[102] EU DIRECTIVE 2001/83/EC of the European Parliament, Official Journal L – 311, 28/11/2004, p. 67 – 128 with subsequent amendments,
http://www.edctp.org/fileadmin/documents/ethics/DIRECTIVE_200183EC_OF_THE_EUROPEAN_PARLIAMENT.pdf
Published:- 10/09/2004, Checked online:- 11/08/2013
[103] EU Directive 2011/62/EU of the European Parliament and of the Council
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:174:0074:0087:EN:PDF
Published:- 01/07/2011, Checked online:- 11/08/2013
[104] EU Commission Directive 2003/94/EC
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:262:0022:0026:EN:PDF
Published:- 14/10/2003, Checked online:- 11/08/2013
[105] EudraLex - Volume 4 Good manufacturing practice (GMP) Guidelines.
http://ec.europa.eu/health/documents/eudralex/vol-4/
Published:- 04/02/2011, Checked online:- 11/08/2013
[106] EU Directive 2001/83/EC of the European parliament and of the Council
http://ec.europa.eu/health/files/eudralex/vol-1/dir_2001_83_cons/dir2001_83_cons_20081230_en.pdf
Published:- 30/12/2008, Checked online:- 11/08/2013

Implementation of the EU Directive 2011/62/EU with the UK now requires Brokers of medical products to register with the MHRA[107], and to fulfil the same requirements as the Medicines Regulations 2012, Sections 44(4,a), 170(1,b). All organisations that participate within the supply chain of medical products are required to retain information concerning personal data of individuals for a minimum of 5 years, thus DPA 1998 as mentioned previously, would apply regarding any breach of such information.

The United States of America (USA) accounted for 41.8% of worldwide sales in 2011[108] and is considered an important market for the United Kingdom. The Food and Drug Administration[109] is the agency that governs approval of medical products in the interests of public health, under the Code of Federal Regulations Title 21 Food and Drugs[110]. Part 11 - Electronic Records; Electronic Signatures (21 CFR 11)[111] defines within section 11.10 control of electronic records in order to retain confidentiality and controlled distribution.

The FDA is empowered by several Acts to apply such regulations, the most important of which is the Federal Food, Drug, and Cosmetic Act (FD&C Act)[112]. Chapter III of the Act[113] details the penalties that can be served, via civil and criminal law clauses, of which the majority of cases are handled through the civil courts unless repeat violations are perpetrated by the same offender. The FDA conducts on-site worldwide visits with regards to organisations exporting medical

[107] MHRA, Registration of Brokers introduced by the Falsified Medicines Directive 2011/62/EU
http://www.mhra.gov.uk/home/groups/es-policy/documents/websiteresources/con224464.doc
Published:- 25/03/2008, Checked online:- 11/08/2013
[108] European Federation of Pharmaceutical Industries and Associations, The Pharmaceutical Industry in Figures, Key Data 2012
http://www.efpia.eu/uploads/Modules/Documents/efpia_figures_2012_final-20120622-003-en-v1.pdf
Published:- 15/06/2012, Checked online:- 11/08/2013
[109] United States, official Food and Drug Administration (FDA) website
http://www.fda.gov/
Checked online:- 11/08/2013
[110] FDA, Medical Devices, Code of Federal Regulations - Title 21
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.10
Last Updated:- 01/04/2013, Checked online:- 11/08/2013
[111] Ibid
[112] FDA, Federal Food, Drug, and Cosmetic Act (FD&C Act)
http://www.fda.gov/regulatoryinformation/legislation/federalfooddrugandcosmeticactfdcact/default.htm
Last Updated:- 05/12/2011, Checked online:- 11/08/2013
[113] FDA, FD&C Act Chapter III: Prohibited Acts and Penalties
http://www.fda.gov/regulatoryinformation/legislation/federalfooddrugandcosmeticactfdcact/fdcactchapteriiiprohibitedactsandpenalties/default.htm
Last Updated:- 08/06/2012, Checked online:- 11/08/2013

products, and failure to comply can lead to the FDA issuing warning letters[114]and if necessary a revocation of licences issued[115].

The third largest pharmaceutical market for the UK is Japan[116] which issued guidance with respect to management of computerised systems, translated into English in 2011[117]. Section 6.14 of the guidance is with respect to Conducting Information Security Management, where it is detailed that organisations are required to make appropriate measures to protect confidentiality. Compliance inspection regarding medical products manufactured by foreign companies is conducted at the relevant manufacturing sites by the Pharmaceuticals and Medical Devices Agency (PMDA)[118].

Pharmaceutical organisations that implement DLP technologies will be better placed to meet these UK & International requirements.

[114] FDA, Inspections, Compliance, Enforcement, and Criminal Investigations, Mediagnost GmbH 08/05/2012 http://www.fda.gov/iceci/enforcementactions/warningletters/2012/ucm308110.htm
Last Updated:- 13/06/2012, Checked online:- 11/08/2013
[115] FDA, Vaccines, Blood & Biologics, Notice of Intent to Revoke (NOIR) Letter: Allergy Laboratories, Inc http://www.fda.gov/biologicsbloodvaccines/guidancecomplianceregulatoryinformation/complianceactivities/administrativeactionsbiologics/ucm344480.htm
Last Updated:- 20/03/2013, Checked online:- 11/08/2013
[116] European Federation of Pharmaceutical Industries and Associations, The Pharmaceutical Industry in Figures, Key Data 2012
http://www.efpia.eu/uploads/Modules/Documents/efpia_figures_2012_final-20120622-003-en-v1.pdf
Published:- 15/06/2012, Checked online:- 11/08/2013
[117] Tentative translation of Guideline on Management of Computerized Systems for Marketing Authorization Holders and Manufacturers of Drugs and Quasi-drugs, not formally authorized by Ministry of Health, Labour and Welfare of Japan
http://www.pmda.go.jp/english/service/pdf/gmp/guideline_for_computerized_systems/20110817.pdf
Published:- 17/08/2011, Checked online:- 11/08/2013
[118] Official website for the Pharmaceuticals and Medical Devices Agency, Japan (English text)
http://www.pmda.go.jp/english/index.html
Checked online:- 11/08/2013

Financial Services legal liabilities

The key pieces of UK financial legislation is the Financial Services and Markets Act 2000[119] (FSMA), Enterprise Act 2002[120], Banking Act 2009[121] (BA), Financial Services Act 2010[122] and more recently the Financial Services Act 2012[123] (FS), which came into force 1st April 2013 introducing a whole series of amendments to previous legislation.

The FS Act has implemented significant changes with respect to financial regulatory authorities[124], where the Financial Services Authority[125] has been divided into two new regulatory authorities, the Financial Conduct Authority (FCA)[126] and The Prudential Regulation Authority (PRA)[127], which is part of the Bank of England[128].

This triage of the FCA, Treasury[129] and Bank of England has the responsibility to ensure financial stability within the UK. The Bank of England has the authority to impose substantial financial penalties[130], under the FSMA 2000 and BA 2009 Acts where penalties are determined by a process of assessing five factors[131] and are not limited by statutory legislation.

---

[119] Financial Services and Markets Act 2000, 2000 Chapter 8, http://www.legislation.gov.uk/ukpga/2000/8/contents, Enacted:- 14/07/2000, Checked online:- 11/08/2013
[120] Enterprise Act 2002, 2002 Chapter 40 http://www.legislation.gov.uk/ukpga/2002/40/contents Enacted:- 07/11/2002, Checked online:- 11/08/2013
[121] Banking Act 2009, 2009 Chater 1, http://www.legislation.gov.uk/ukpga/2009/1/contents Enacted:- 12/12/2009, Checked online:- 11/08/2013
[122] Financial Services Act 2010, 2010 Chapter 28, http://www.legislation.gov.uk/ukpga/2010/28/contents Enacted:- 08/14/2010, Checked online:- 11/08/2013
[123] Financial Services Act 2012, 2012 Chapter 21, http://www.legislation.gov.uk/ukpga/2012/21/contents/enacted Enacted:- 19/12/2012, Checked online:- 11/08/2013
[124] HM Treasury, Creating stronger and safer banks http://www.hm-treasury.gov.uk/fin_financial_services_bill.htm Last Updated:- 17/07/2013, Checked online:- 11/08/2013
[125] National Archive of Financial Services Authority website http://webarchive.nationalarchives.gov.uk/*/http:/www.fsa.gov.uk/ Last Updated:- 26/06/2013, Checked online:- 11/08/2013
[126] Financial Conduct Authority, official website, www.fca.org.uk, Checked online:- 11/08/2013
[127] Bank of England, Prudential Regulation Authority, official website http://www.bankofengland.co.uk/pra/Pages/about/default.aspx , Checked online:- 11/08/2013
[128] Bank of England, official website, http://www.bankofengland.co.uk/Pages/home.aspx Checked online:- 11/08/2013
[129] HM Treasury, official website, https://www.gov.uk/government/organisations/hm-treasury Last Updated:- 09/08/2013, Checked online:- 11/08/2013
[130] Bank of England, Policy statement, Financial penalties imposed by the Bank http://www.bankofengland.co.uk/financialstability/Documents/fmi/penalties.pdf Published:- 11/04/2013, Checked online:- 11/08/2013
[131] Ibid

Financial services organisations are under close scrutiny for market abuse[132], especially with regards to the disclosure of information. The FSMA 2000 Act Section 118 (3)[133] specifically covers the circumstance of someone passing information to another person that would be considered unacceptable as per the obligations of their position. This person would be considered an insider, as explained with Section 118B[134] of the FSMA 2000 Act.

The FCA's handbook has a section on Market Conduct[135] that provides guidelines on what is defined as "improper disclosure"[136] with regards to current legislation. The examples cited are within a "social context", where such a breach could also occur via email.

The FCA handbook for Disclosure and Transparency Rules (DTR) explains the reasons regarding why insider information may be delayed[137] without breaching the Market Abuse EU Directive 2003/6/EC[138], however in the main inside information must be disclosed to a Regulated Information Service (RIS)[139] as quickly as possible (DTR 2.2.1[140]).

---

[132] Pinsent Masons article, City sackings and suspensions at a five-year high,
http://www.out-law.com/en/articles/2013/january/city-sackings-and-suspensions-at-a-five-year-high/
Published:- 14/01/2013, Checked online:- 11/08/2013
[133] Financial Services and Markets Act 2000, Part VIII Market abuse, Section 118 (Market Abuse)
http://www.legislation.gov.uk/ukpga/2000/8/section/118
Last Updated:- 31/12/2011, Checked online:- 11/08/2013
[134] Financial Services and Markets Act 2000, Part VIII Market abuse, Section 118B (Insiders)
http://www.legislation.gov.uk/ukpga/2000/8/section/118B
Last Updated:- 01/07/2005, Checked online:- 11/08/2013
[135] Bank of England, Prudential Regulation Authority, Market Conduct
http://media.fshandbook.info/content/full/MAR.pdf , Published:- 02/08/2013, Checked online:- 11/08/2013
[136] Bank of England, Prudential Regulation Authority, MAR 1.4 Market abuse (improper disclosure)
http://media.fshandbook.info/content/full/MAR/1/4.pdf
Published:- 02/08/2013, Checked online:- 11/08/2013
[137] Financial Conduct Authority, Disclosure Rules and Transparency Rules (DTR), Legitimate interests and when delay will not mislead the public
http://fshandbook.info/FS/html/FCA/DTR/2/5#D126
Last Updated:- 01/04/2013, Checked online:- 11/08/2013
[138] EU Directive 2003/6/EC, insider dealing and market manipulation (market abuse)
http://www.esma.europa.eu/system/files/Dir_03_6.pdf
Published:- 12/04/2003, Checked online:- 11/08/2013
[139] Financial Conduct Authority, "Make a regulatory announcement"
http://www.fca.org.uk/firms/markets/ukla/information-dissemination/announcement
Published:- 31/03/2013, Checked online:- 11/08/2013
[140] Financial Conduct Authority, Disclosure Rules and Transparency Rules (DTR), Requirement to disclose inside information
http://fshandbook.info/FS/html/FCA/DTR/2/2
Published:- 01/04/2013, Checked online:- 11/08/2013

The offence of improper disclosure with regards to Market Abuse can lead to individuals being handed large fines for breach of the legislation, such as in the case of Ian Hannam[141]. At the time of the offence being committed Ian Hannam was Global Co-Head of UK Capital Markets at JP Morgan Cazenove, and he had sent emails which proved he had passed insider information which he failed to disclose to a RIS. As a result the FSA determined that Ian Hannam had breached FSMA 2000 regarding several sub-sections of 118 regarding Market Abuse and was fined £450,000.00.

Organisations such as the London Stock Exchange plc[142] qualify as a Recognised Investment Exchange[143] (RIE) under Part XVIII of FSMA 2000[144], and are exempt from general prohibition of the act in accordance with activity conducted by a RIE. To achieve exemption RIEs are required to fulfil a risk based assessment of the organisation including operational and other risks[145]. Section REC 2.3.20 (2)[146] of the FCA handbook advises that RIEs must have sufficient provision to mitigate risk of data loss and leakage, as part of the financial risk assessment and operational risk buffer.

The Alternative Investment Fund Managers EU Directive 2011/61/EU[147] has been transposed into UK National law via Alternative Investment Fund Managers (AIFM) Regulations 2013[148] which came into force on the 22nd July 2013.

---

[141] Practical Law, Market abuse: FSA decision notice for improper disclosure
http://uk.practicallaw.com/0-518-7926?q=email+insider+information#null
Published:- 03/04/2012, Checked online:- 11/08/2013
[142] London Stock Exchange, Official website
http://www.londonstockexchange.com/
Checked online:- 11/08/2013
[143] Financial Conduct Authority, Recognised Investment Exchanges
https://www.fsa.gov.uk/register/exchanges.do
Last Updated:- 11/08/2013 Checked online:- 11/08/2013
[144] Financial Services and Markets Act 2000, Part XVIII, Recognised Investment Exchanges and Clearing Houses
http://www.legislation.gov.uk/ukpga/2000/8/part/XVIII
Checked online:- 11/08/2013
[145] Financial Conduct Authority Handbook, Recognised Investment Exchanges, REC 2.3.6, Operational and other risks
http://fshandbook.info/FS/html/FCA/REC/2/3
Published:- 01/04/2013, Checked online:- 11/08/2013
[146] Ibid REC 2.3.20 (2)
[147] EU Directive 2011/61/EU, on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:174:0001:0073:EN:PDF

The European Securities and Markets Authority (ESMA)[149] has issued technical advice with respect to implementing measures of the AIFM directive[150]. The report makes recommendations that adequate arrangements should be implemented to prevent the misuse and disclosure of confidential information[151].

The EU Capital Requirements Directive IV[152] (CRD) and associated Capital Requirements Regulations (CRR)[153] as of 17th July 2013 introduced new measures, especially with regards to financial organisations retaining sufficient capital to loans and potential losses on investments. The directive is to be incorporated within UK National Law, the timetable and implementation is yet to be confirmed in detail[154]. The implication of CRD and CRR is that improper disclosure of information may require institutions to retain greater capital reserves to cover investment risks, resulting in being less competitive within the capital markets.

Published:- 01/07/2011, Checked online:- 11/08/2013

[148] Draft Statutory Instrument, 2013 No. 0000, Financial Services and Markets, TheAlternative Investment Fund Managers Regulations 2013
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/198211/aifm_regulations_090513.pdf
Published:- 09/05/2013, Checked online:- 11/08/2013

[149] European Securities and Markets Authority (ESMA), Official website
http://www.esma.europa.eu
Checked online:- 11/08/2013

[150] Final Report, ESMA's technical advice to the European Commission on possible implementing measures of the Alternative Investment Fund Managers Directive, Ref: ESMA/2011/379
http://www.esma.europa.eu/system/files/2011_379.pdf
Published:- 16/11/2011, Checked online:- 11/08/2013

[151] Ibid page 105

[152] European Commission, The EU Single Market, Capital Requirements Directive: Legislation in force
http://ec.europa.eu/internal_market/bank/regcapital/legislation_in_force_en.htm
Published:- 17/07/2013, Checked online:- 11/08/2013

[153] European Parliament News, EU Bank Capital Requirements Regulation and Directive, REF: 20130412BKG07195
http://www.europarl.europa.eu/news/en/pressroom/content/20130412BKG07195/html/EU-Bank-Capital-Requirements-Regulation-and-Directive
Published:- 15/04/2013, Checked online:- 11/08/2013

[154] Bank of England, Prudential Regulation Authority, Consultation Paper CP5/13, Strengthening capital standards: implementing CRD IV
http://www.bankofengland.co.uk/pra/Documents/publications/policy/2013/implementingcrdivcp513.pdf
Published:- 02/08/2013, Checked online:- 11/08/2013

The topic of personal data protection was covered in detail within a FCA (formerly the FSA) report[155] referring to the legislative requirements of DPA 1998[156]that financial firms must adhere to.

The implementation of DLP technologies within the financial industry is no doubt a high priority given the potential commercial and legal consequences of unauthorised data leaving the organisation.

Industry Regulation

There are industry standards and regulations such as ISO[157], BS[158] that although not governed under legal legislation, still require compliance if organisations wish to operate within specific industries.

Credit & Debit Card Industry

The Payment Card Industry Security Standards Council[159] (PCI SSC) was founded in 2006 by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The PCI SSC defines the PCI security standard, but neither validates or enforces compliance, the responsibility of which is upon the card issuer. MasterCard sets out within its rules[160]that merchants that fail to comply can be issued fines up to $100,000.00 (USD)[161] for each noncompliance violation and up to $0.50 (USD) for each card affected as a result of a security breach. Visa has a minimum fine of $100,000.00 (USD)[162], for each data breach

[155] Financial Services Authority, Data Security in Financial Services
http://www.fsa.gov.uk/pubs/other/data_security.pdf
Published:- 23/08/2008, Checked online:- 11/08/2013
[156] Ibid Section 2.6.1
[157] International Organization for Standardization, official website
http://www.iso.org/iso/home.html
Checked online:- 11/08/2013
[158] The British Standards Institution, official website
http://www.bsigroup.co.uk
Checked online:- 11/08/2013
[159] PCI Security Standards Council, LLC, official website
https://www.pcisecuritystandards.org/
Checked online:- 11/08/2013
[160] MasterCard Worldwide, MasterCard Rules
http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf
Published:- 14/07/2013, Checked online:- 11/08/2013
[161] Ibid Section 3.1.2
[162] VISA, If Compromised
http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html

incident, which can rise to $500,000 (USD) if found to be non-complaint of PCI Data Security Standard (DSS)[163] at the time of the breach.

Section 1.3.5 of PCI DSS requires organisations not to allow unauthorised outbound traffic that can contain card data to reach the internet, and this is where DLP technologies can assist to facilitate this requirement.

Copy Right and Intellectual Property Protection

Organisations place a large value upon information assets, which have been typically created by investing large amounts of time, finance and expertise. Organisations will seek to use appropriate legal mechanisms to protect their information assets, and in the event of information being misappropriated, how best to seek restitution.

The primary UK legislation that empowers organisations to protect their Intellectual Property Rights (IPR) is the Copyright, Designs & Patents Act 1988[164]. This legislation has been amended since it came into force, mostly due to EU legislation and subsequent UK legislation as detailed by the Intellectual Property Office (IPO)[165] within a document that explains Copyright with respect to Rights Performances, Publication Right and Database Right[166]. It is important to understand with regards to the applicable copyright legislation that DLP technology can be used to protect an organisation's interests and assert its rights where necessary.

Checked online:- 11/08/2013

[163] Payment Card Industry (PCI), Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0
https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
Published:- 29/08/2011, Checked online:- 11/08/2013

[164] Copyright, Designs and Patents Act 1988, 988 Chapter 48
http://www.legislation.gov.uk/ukpga/1988/48/contents
Enacted:- 15/11/1998, Checked online:- 11/08/2013

[165] Intellectual Property Office, official website
http://www.ipo.gov.uk/ , Checked online:- 11/08/2013

[166] Copyright Rights in Performances Publication Right, Database Right. Unofficial consolidated text of UK Legislation to 3 May 2007
http://www.ipo.gov.uk/cdpact1988.pdf , Published:- 15/09/2011, Checked online:- 11/08/2013

Database information

Most organisations retain digital information which would be considered under UK Law as a database[167]. The Copyright and Rights in Databases Regulations 1997[168], affords intellectual property protection of such databases, where organisations typically have invested time, money and effort with regards to populating the database with information.

The UK Regulations were implemented as per EU Directive 96/9/EC[169], which provides "sui generis"[170] protection to information contained within a database. The extraction and reuse of such data from a database is considered a breach of the Regulations and Directive.

The subtly of the regulation is not directly regarding the nature of the data itself, but the rights of extracting and reusing that data without licence from the database owner. The Crowson Fabrics Ltd v Rider legal case[171] highlighted the importance of differentiation between the data (which was considered not confidential) to the actions of the ex-employees who had copied the data, thus infringing the copy work rights of their ex-employer.

The use of DLP technology can provide valuable evidence to show that database information was illegally acquired an important consideration if a search and seizure order is made against the defendant. If such an order is to be issued, such evidence will no doubt demonstrate to the courts when the defendant took information, and possibly what the content of that information was.

Computer Software

Copyright and Computer Software is a very contentious area of law, as the current legislation has a very narrow scope on what would be considered a breach of copyright. The EU Directive

[167] The Copyright and Rights in Databases Regulations 1997, PART II Regulation 6
http://www.legislation.gov.uk/uksi/1997/3032/regulation/6/made
Checked online:- 11/08/2013
[168] The Copyright and Rights in Databases Regulations 1997, Statutory Instruments 1997 No. 3032
http://www.legislation.gov.uk/uksi/1997/3032/contents/made
Came into force:- 01/01/1998, Checked online:- 11/08/2013
[169] EU Directive 96/9/EC, on the legal protection of databases
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1996:077:0020:0028:EN:PDF
Published:- 27/03/1996, Checked online:- 11/08/2013
[170] Ibid, Articles 18 & 19
[171] Crowson Fabrics Limited v Paul Rider, Warren Stimson, Concept Textiles Limited [2007] EWHC 2942 (Ch)

2009/24/EC on the legal protection of computer programs[172] explains that only the only the expression of a computer program is protected[173], and the underlying programming languages and the development of applications is not.

This point was covered within the legal case of SAS Institute Inc. v World Programming Ltd[174], where it was determined that there was no breach of copyright with respect to the development of software by World Programming as there was no "literal" copying of the software, more a facsimile of the SAS product. Computer "source code" that is taken from one application and used within another is considered breach of copyright as determined in the case of Cantor Fitzgerald International v Tradition (UK) Ltd[175], where portions of source code was found to have been copied. Proceedings were started based upon a determination by the plaintiff that the time frame by which software was developed by the defendant(s) was impossible. Therefore initially there was no evidence to make the accusation, rather circumstantial facts leading to suspicions that copying of source code did occur.

This case occurred over a decade ago, and such a justification today would prove more difficult to establish, especially with the advent of Rapid Application Development (RAD) frameworks. Whereas DLP technology can detect when source code left the organisation, the method by which this occurred (email, file copy, upload to website etc), who performed the act providing factual evidence that an organisation can use to support their case.

Computer Aided Design drawings

Computer Aided Design (CAD) drawings are used by many organisations in order to facilitate the delivery of services, manufactured goods, construction etc. The creation of CAD drawings takes a high level of expertise and time, and therefore is considered a valuable asset to be protected by contractual agreements and copyright. In the case of Force India Formula One

[172] EU Directive 2009/E/EC on the legal protection of computer programs
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF
Published:- 05/05/2009, Checked online:- 11/08/2013
[173] Ibid Section 11
[174] SAS Institute Inc. v World Programming Ltd [2013] EWHC 69 (Ch) - 25/01/13
[175] Fitzgerald International v Tradition (UK) Ltd [2000] R.P.C. 95; [1999] Masons C.L.R. 157

Team Ltd v 1 Malaysia Racing Team Sdn Bhd[176], an employee of the defendant copied data (mostly CAD files) from the plaintiff's server onto an external hard drive and later used those files without the plaintiff's permission.

The case determined there was a breach of UK copyright legislation, where the CAD files were considered to be both artistic and literary works. It only came to the plaintiff's attention that the CAD files had been stolen when a press release regarding a new relationship between the defendant and Lotus F1 Racing[177] , featured designs which the plaintiff recognised to be a copy of their own product. If the defendant had not been so blatant regarding the copying of design, the plaintiff may never have realised that the CAD files had been copied. DLP technology would have been able to either prevent the copying of files at least alert the plaintiff that CAD drawings had been misappropriated in order to minimise the commercial impact of such theft.

Data Loss Prevention Summary

DLP technology is about preventing electronic data from leaving the organisation, unless required under normal operational circumstances. The greatest risk for data to be misappropriated originates internally, and the consequences both to the organisation's reputation, commercial interests and legal repercussions can be substantial. There are clear justifications on why organisations would implement DLP technologies; but what authority do they have with respect to including devices used under a BYOD programme?

[176] Force India Formula One Team Ltd v 1 Malaysia Racing Team Sdn Bhd [2012] EWHC 616 (Ch); [2012] R.P.C. 29;

[177] AOL Inc, Autoblog, Press Release, Malaysian-backed Lotus F1 Racing gears up for 2010 http://www.autoblog.com/2009/10/16/malaysian-backed-lotus-f1-racing-gears-up-for-2010/ Published:- 14/10/2009, Checked online:- 11/08/2013

Bring Your Own Device (BYOD) Who, What, Why and When?

Traditionally organisations had complete control regarding what employees were allowed to use with respect to Information Communication Technology (ICT) and followed the approach of "Use what you are told" (UWYT). However with the ability for individuals to easily connect via telecommunication infrastructure, and the increasing sophistication of user's own personal devices, the practice of "Bring you own device" (BYOD), or "Bring your own technology" (BYOT) is more commonplace. Given the challenges of BYOD with respect to supporting connectivity, security, operations etc, why are organisations supporting this technological framework?

Work in the modern enterprise has metamorphosed from location based to ongoing activity that is location independent[178], with employees demanding the ability to use their own devices for work purposes[179]. The business advantages for organisations to leverage employee's personal devices to allow them access to work related information and systems has shown to increase both efficiency and productivity[180]. Employees have greater flexibility and motivation[181]by virtue of having greater autonomy over their work environment[182]. But BYOD removes the clear delimitation between when employees are at work and when they are not. This presents challenges with respect to The Working Time Regulations 1998[183] (WTR 1998), where unless

[178] Friendly Takeover – The consumerization of corporate IT. Booz & Co. Bernnat,R.,O. Acker,N. Bieber, and M. Johnson (2010).
http://www.booz.com/media/uploads/FriendlyTakeoverVPFINAL.pdf
Published:- 26/04/2010, Checked online:- 11/08/2013
[179] B.Y.O.D. Genie Is Out Of the Bottle – "Devil Or Angel", Ms Niharika, Journal of Business Management & Social Sciences Research (JBM&SSR) ISSN No 2319-5614 Volume 1, No. 3,
http://www.borjournals.com/Research_papers/Dec_2012/1060%20%20M.pdf
Published:- 14/12/2012, Checked online:- 11/08/2013
[180] BYOD Gives Competitive Advantage, Say IT Managers. PR Newswire US, http://www.prnewswire.com/news-releases/byod-gives-competitive-advantage-say-it-managers-151687995.html Published:- 16/05/2012, Checked online:- 17/07/2013
[181] ERCIS, Towards an IT Consumerization Theory – A Theory and Practice Review, Bjorn Niehaves, Sebastian Koffer, Kevin Ortbach, Stefan Katschewitz
http://www.ercis.org/sites/default/files/publications/2012/ercis_working_report_13_-_consumerization_0.pdf
Published:- 07/2012, Checked online:- 11/08/2013
[182] Ibid
[183] The Working Time Regulations 1998, Statutory Instrument 1998 No. 1833
http://www.legislation.gov.uk/uksi/1998/1833/contents/made
Came into force:- 01/10/1998, Checked online:- 11/08/2013

employees opt-out, the maximum number of working hours allowed is forty eight[184]. These hours include overtime and on-call (MacCartney v Oversley[185]), therefore having BYOD effectively enables 24 access to employees via their personal devices, and this will present a challenge, establishing whether employees are under pressure to respond to communications (emails and text messages) outside typical work hours. The UK legislation adopts the European Working Time Directive 2003/88/EC[186] (EWTD), however the UK is the only country in Europe that allows employees to opt-out of the 48 hour restriction[187]. This opt-out stems from the UK culture or working long hours[188]and studies have shown that UK employees have been coerced to agree to opting-out[189]. Regarding BYOD programs, cases have been brought to the courts in the USA with respect to employees suing their employers for unpaid overtime hours based upon usage of their smart phones[190].

BYOD/BYOT applies to the whole range of devices, smart phones, table devices, personal computers and laptops, providing access for both home workers and the mobile work force. The trend for BYOD to be used more within organisations is such that Gartner predicts 50% of businesses will require employees to participate within a business BYOD programme by 2017[191].

---

[184] The Working Time Regulations 1998, PART II Regulation 4, Maximum weekly working time
http://www.legislation.gov.uk/uksi/1998/1833/regulation/4/made
Checked online:- 11/08/2013

[185] MacCartney v Oversley House Management, Employment Tribunal, 31 January 2006 [2006] I.C.R. 510; [2006] I.R.L.R. 514

[186] EU Directive 2003/88/EC concerning certain aspects of the organisation of working time
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:299:0009:0019:EN:PDF
Published:- 18/11/2003, Checked online:- 11/08/2013

[187] The Working Time Regulations 1998, PART IV Regulation 35, Restrictions on contracting out
http://www.legislation.gov.uk/uksi/1998/1833/regulation/35/made
Checked online:- 11/08/2013

[188] Opting out of the 48-hour week – Employer Necessity or Individual Choice? An Empirical Study of the operation of Article 18(1)(B) of the Working Time Directive in the UK, Catherine Barnard, Simon Deakin and Richard Hobbs,
http://www.cbr.cam.ac.uk/pdf/wp282.pdf, Published:- 15/04/2004, Checked online:- 11/08/2013

[189] Long working hours and health status among employees in Europe: between-country differences, Artazcoz L, Cortes I, Escriba-Aguir V, Bartoll X, Basart H,
http://www.researchgate.net/publication/233798254_Long_working_hours_and_health_status_among_employees_in_Europe_between-country_differences/file/d912f50bdef2ed6ada.pdf,
Published:- 03/12/2012, Checked online:- 28/07/2013

[190] Smartphones and the Fair Labor Standards Act, By Spencer H. Silverglate and Craig Salner,
http://cspalaw.com/pdf/Smartphones.pdf, Published:- 01/06/2011, Checked online:- 11/08/2013

[191] Gartner Press Release, Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes
http://www.gartner.com/newsroom/id/2466615
Published:- 01/05/2012, Checked online:- 11/08/201

However BYOD requires employee's voluntary acceptance to participate within such programmes, changing the relationship between employees and the use of personally owned technology to facilitate their role within the organisation[192]. Despite the known benefits of BYOD to both organisations and employees, there is no doubt there are concerns on the behalf of employees with respect to the security, privacy and legal considerations for using their own device for work purposes.

Therefore although BYOD can provide flexibility and empowerment with respect to employee connectivity and can also provide better business continuity, leading to increased job satisfaction[193] this introduces several challenges as previously mentioned the most important being security[194]; perhaps this is why BYOD is sometimes referred to as "Bring your own disaster"[195].

[192] ERCIS, Towards an IT Consumerization Theory – A Theory and Practice Review, Bjorn Niehaves, Sebastian Koffer, Kevin Ortbach, Stefan Katschewitz http://www.ercis.org/sites/default/files/publications/2012/ercis_working_report_13_-_consumerization_0.pdf Published:- 07/2012, Checked online:- 11/08/2013

[193] Employee Attitudes and Job Satisfaction, Human Resource Management, Winter 2004, Vol 43, No 4, Pages 395-407, Lise M. Saaria and Timothy A. Judge, http://utm.edu/staff/mikem/documents/jobsatisfaction.pdf, Published:- 02/12/2004, Checked online:- 20/07/2013

[194] Bring your own device, Agility through consistent delivery, PwC http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/byod-1-25-2012.pdf Published:- 25/01/2012, Checked online:- 11/08/2013

[195] Make sure BYOD doesn't mean Bring Your Own Disaster, Scott Reeves, http://www.techrepublic.com/blog/data-center/make-sure-byod-doesnt-mean-bring-your-own-disaster/, Published:- 15/02/2013, Checked online:- 28/07/2013

Employee attitude towards privacy and security

Employee uncertainty with respect to using locally installed applications on their personal device to access online information is primarily influenced by concerns around privacy and security[196]. First focussing on privacy concerns, a study conducted by Pew Research Center[197]indicated that 57% of individuals surveyed had removed, or refused to install an application on their personal device because of concerns of disclosing personal information. The European Article 29 data protection working party released an opinion with respect to applications on smart devices regarding data protection[198] that highlighted the concerns over the lack of transparency with respect to application access to personal information, informed consent and the use of information collected adhering to the principle of data minimisation. The working party concluded that the principle of "privacy by design"[199]should be applied throughout all layers of infrastructure from telecommunications companies, hardware vendors, operating system developers, all the way through to the installed applications.

There have been cases of where the operations of applications have breached data protection legislation, such as the Whatsapp[200] and Facebook[201]applications. Concerns were raised by the Dutch and Canadian authorities with respect to the Whatsapp application gaining access to the user's entire device address book (contacts)[202] without users informed consent and ignoring the

[196] Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal Agent Perspective, MIS Quarterly Vol 31 No 1 Pages 105-136 Paul A. Pavlou, Huigan Liang, Yajion Xue, http://im1.im.tku.edu.tw/~myday/teaching/992/SEC/S/992SEC_T5_Paper_20100415_UNDERSTANDING%20AND%20MITIGATING%20UNCERTAINTY%20IN%20ONLINE%20EXCHANGE%20RELATIONSHIPS.pdf, Published:- 03/2007, Checked online:- 11/08/2013

[197] Privacy and Data Management on Mobile Devices, Jan Lauren Boyles, Aaron Smith and Mary Madden, http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf Published:- 05/09/2012, Checked online:- 20/07/2013

[198] Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, Published:- 14/03/2013, Checked online:- 20/07/2013

[199] Ibid page 11

[200] WhatsApp Inc official website http://www.whatsapp.com/ Checked online:- 11/08/2013

[201]Facebook, official website https://www.facebook.com/ , Checked online:- 11/08/2013

[202] Office of the Privacy Commissioner of Canada, News Release, WhatsApp's violation of privacy law partly resolved after investigation by data protection authorities, Anne-Marie Hayden http://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp Published:- 28/01/2013, Checked online:- 11/08/2013

principle of data minimisation. Facebook released an update in February 2013 for their Android application, which was found to upload user's phone number before they had even opened the application on their device[203]. Such instances only compound public mistrust with respect to installing applications onto their personal devices. This lack of trust is also pervasive with respect to employer BYOD programmes, where a report by Aruba Networks[204]showed an average of 16.3% of those surveyed have not informed their employer about using their personal device for work, citing privacy concerns. The report also indicated that approximately 50% of those surveyed would be "angry" if the IT department gathered personal information from user's own devices, with an average of 44.6% responding they would feel "violated" if they knew such data was had been collected. The report also shows that because of this lack of trust, organisations are at risk with respect to data breaches and "non-sanctioned" use of personal devices, where the reports states that an average of 16.6% of respondents would not report to their employer if their device had been compromised. Even if those respondents thought there was a work related data leak, 66% would not immediately report the leak immediately, with 19% stating they would never disclose such a data leak. A survey conducted by TNS Infratest on behalf of Kaspersky[205] showed that 29% of respondents surveyed indicated there would be half a day before a data loss would be reported by employees; this introduces the topic of security and employee commitment to adhering to company security policies when using their personal device. Employee's perception of security can be explained by what threat is placed against the information assets held within the organisation[206], and the fear or concern this creates within the employee as a result. Organisations can implement technologies that have complete control over personal devices, restricting what users can and cannot including install additional applications

[203] The Huffington Post, Facebook Android App Collects Phone Numbers Without Permission -- Even From Non-Members, Bianca Bosker
http://www.huffingtonpost.com/2013/06/28/facebook-android-app-phone-numbers_n_3518652.html
Published:- 28/06/2013, Checked online:- 11/08/2013

[204] Employees tell the truth about your company's data; How to make mobile devices safe for work and play, Aruba Networks
http://www.arubanetworks.com/pdf/solutions/EB_mdmreport.pdf,
Published:- 10/07/2013, Checked online:- 11/08/2013

[205] TNS Infratest, Kaspersky Lab PR Survey 2013 - Netherlands
http://newsroom.kaspersky.eu/fileadmin/user_upload/nl/Campaign/KESB2013/Misc/Report_NL_Kaspersky_Lab_2013.pdf, Published:- 15/03/2013, Checked online:- 11/08/2013

[206] Protection motivation and deterrence: a framework for security policy compliance in organisations, European Journal of Information Systems (2009) 18, pages 106-125, Tejaswini Heratch and H. Raghav Rao,
http://www.som.buffalo.edu/isinterface/papers/ejis20096.pdf,
Published:- 27/05/2009, Checked online:- 20/07/2013

etc. However implementing such security features onto user's personally owned devices will probably be met with resistance as such control over personal property is unlikely to be tolerated. This is where security divergence starts to emerge between BYOD and UWYT, as control is divested away from the employer, and employees become more responsible for the data held on their personal device.

BYO Big Brother – sanctioning surveillance

Can BYOD programmes install surveillance DLP technologies without employee's knowledge? George Orwell's novel "1984"[207] describes a society where its citizens are under the state's constant scrutiny. This is quite apt in lieu of the recent disclosure of the NSA secret surveillance program (Prism) as mentioned earlier, which has resulted in a huge surge of sales of the book[208]. The concerns of a "surveillance society" was documented within a House of Lords report[209] which discusses the danger of "sleep walking into a surveillance society"[210] and the role of the citizen, especially with regards to the doctrine of "informational self-determination"[211], which empowers individuals to have control over their own private data. The legal concept of "informational self-determination" can be attributed a 1983 legal case in Germany where the government wanted to enact the Population Census Act, which was annulled by the Bundesverfassungsgericht (German Federal Constitutional Court) as being partly unconstitutional[212]. The decision of the Bundesverfassungsgericht set the basis of German data

[207] The Literature Network, George Orwell, 1984, Summary Part 1, Chapter 1
http://www.online-literature.com/orwell/1984/2/
Checked online:- 11/08/2013
[208] The Guardian Book Blog, George Orwell back in fashion as Prism stokes paranoia about Big Brother, Stephen Moss
http://www.guardian.co.uk/books/booksblog/2013/jun/11/george-orwell-prism-big-brother-1984
Published:- 11/06/2013, Checked online:- 11/08/2013
[209] House of Lords, Constitution Committee - Second Report, Surveillance: Citizens and the State
http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm
Published:- 21/01/2009, Checked online:- 11/08/2013
[210] House of Lords, Constitution Committee - Second Report, Surveillance: Citizens and the State, Chapter 8: the role of Citizens
http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1810.htm
Published:- 21/01/2009, Checked online:- 11/08/2013
[211] Ibid
[212] Computer Law & Security Report, Volume 25, Issue 1, 2009, Pages 84-88, Data protection in Germany I: The population census decision and the right to informational self-determination, Gerrit Hornung & Christoph Schnabel
http://cms.uni-kassel.de/unicms/fileadmin/groups/w_030405/Ehemalige_Mitarbeiter/Dr._Christoph_Schnabel/Hornung___Schnabel__Data_protection_in_Germany_I__CLSR_2009__84.pdf
Published:- 2009, Checked online:- 11/08/2013

protection legislation, which has been referred on a regular basis within subsequent cases. The idea of informational self-determination is part of the general personality right, which is the concept that individuals are free to develop their own self determined personality[213]. This legal concept was relied upon when the German law enforcement authorities wanted to secretly install software on to suspect's computers for the purpose of covert intelligence gathering, the right of which was to be provided under the North Rhine-Westphalia Constitution Protection Act of 2006. This act was ruled unconstitutional by the Constitutional Court as it failed to protect individual's right informational self-determination[214]. The use of covert state surveillance can be considered a world wide threat to the human right of privacy as indicated within a recent United Nations report[215] that makes several recommendations in order individuals rights to privacy are preserved and protected within a proper legal framework. The technology for covert surveillance of mobile devices is ubiquitous[216], and it appears the US government has become the largest purchaser of such software as reported by Reuters[217]. The position within the UK is that state sanctioned covert investigation can be facilitated by intrusive surveillance[218] under RIPA[219], authorised by the home secretary, chief constable, designated officials from the Serious Organised Crime Agency (SOCA), designated officials from HMRC and the chairman of the Office of Fair Trading, with provisions that in the absence of the chief constable etc, other senior

[213] Ibid
[214] Federal Constitutional Court, 1BvR 370/07, 27.2.2008, paragraph no. (1 - 333)
http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
Published:- 27/02/2008, Checked online:- 11/08/2013
[215] United Nations, General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue
http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
Published:- 15/04/2008, Checked online:- 11/08/2013
[216] The SmartPhone Who Loved Me: FinFisher Goes Mobile?, Morgan Marquis-Boire, Bill Marczak and Claudio Guarnieri,
https://citizenlab.org/wp-content/uploads/2012/08/11-2012-thesmartphonewholovedme.pdf,
Published:- 08/2012, Checked online:- 28/07/2013
[217] Special Report: U.S. cyberwar strategy stokes fear of blowback, Joseph Menn,
http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510,
Published:- 10/05/2013, Checked online:- 28/07/2013
[218] Home Office, Covert Surveillance and Property Interference, Revised Code of Practice
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf
Published:- 17/03/2010, Checked online:- 11/08/2013
[219] Regulation of Investigatory Powers Act 2000, 2000 Chapter 23
http://www.legislation.gov.uk/ukpga/2000/23/contents
Enacted:- 28/07/2000, Checked online:- 11/08/2013

staff can authorise such surveillance[220]. The Protection of Freedoms Act 2012 adds safeguards for certain surveillance under RIPA[221] requiring authorisations to have proper judicial approval to ensure the use of covert surveillance is proportionate with respect to the detection and recording of illegal activity. Outside of law enforcement and security services, organisations are expected to provide clear policies explaining how monitoring will be implemented, an example of which is published by Bristol University[222]. The university's policy is very specific with regards to being authorised to access any IT facilities owned by the university; however this doesn't address the scenario of BYOD. Note covert surveillance of employees is not prohibited as in the case of City and County of Swansea v Mr D A Gayle[223], but the employer must be in the position to legally justify the use of covert monitoring otherwise risk breaching ECHR-L.

Legal liabilities regarding BYOD

The ICO published on the 13th March 2013 guidance[224] with respect to an organisation's responsibility to adhere to DPA 1998[225] when employees use their own device. The guidance focuses on Principle 7 of the DPA, which requires the data controller to "maintain appropriate technical and organisational measures to protect personal data against accidental, loss, destruction or damage of personal data"[226]. Thus the onus is upon the organisation being the data controller to ensure there isn't a breach of DPA 1998, regardless of ownership of the device

[220] Regulation of Investigatory Powers Act 2000, Part II Authorisation of surveillance and human intelligence sources, Section 32, Authorisation of intrusive surveillance.
http://www.legislation.gov.uk/ukpga/2000/23/section/32
Checked online:- 11/08/2013
[221] Protection of Freedoms Act 2012, 2012 Chapter 9,
http://www.legislation.gov.uk/ukpga/2012/9/enacted
Enacted:- 01/05/2012, Checked online:- 11/08/2013
[222] University of Bristol Information Security Policy
http://www.bristol.ac.uk/infosec/policies/docs/isp-18.pdf
Published:- 08/01/2013, Checked online:- 11/08/2013
[223] City and County of Swansea v Mr D A Gayle, Appeal No. UKEAT/0501/12/RN, 16 April 2013
[224] ICO, DPA 1998, Bring your own device (BYOD)
http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.pdf
Published:- 13/03/2013, Checked online:- 11/08/2013
[225] Data Protection Act 1998, 1998 CHAPTER 29,
http://www.legislation.gov.uk/ukpga/1998/29/contents,
Enacted 16/071998, Checked online: -11/08/2013
[226] Data Protection Act 1998, Schedule 1Part I Section 7
http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/paragraph/7
Checked online: -11/08/2013

used to process the data[227]. The guidance states that the organisation will need to assess the potential of data leakage and BYOD, therefore the use of DLP technology would be appropriate. Organisations must have employee's "freely given"[228] consent to implement DLP technology on their device, in order not to contravene the DPA 1998 or the Computer Misuse Act 1990[229] (CMA). The CMA provides no definition for the term computer, thus Smartphones, tablet devices as well as laptops can be considered to meet the definition of a computer.

It is important to note that the ICO's guidance makes reference to an acceptable user policy[230], and user's responsibilities, which includes a reference to the employment practices code[231]explaining that organisations need to clearly explain, employees are legally entitled to privacy with respect to their personal lives not directly involved with their employment. The ICO's employment practices code advises that if organisations are to monitor employee activity, it must not contravene Article 8 of the European Convention on Human Rights (ECHR-L)[232] "Everyone has the right to respect for his private and family life, his home and his correspondence". Carmarthenshire College lost a legal case with respect to this legislation, when it was determined by the European Court of Human Rights (ECHR-C) that the college had breached the rights of an employee Lynette Copland[233]because her personal communications were being monitored without warning her in advance. During the case, it was noted by the

[227] ICO, DPA 1998, Bring your own device (BYOD)
http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.pdf, Page 4, Paragraph 3
Published:- 13/03/2013, Checked online:- 11/08/2013

[228] ICO, Data Protection, The employment practices code
http://www.ico.org.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/the_employment_practices_code.ashx, Page 63
Published:- 21/11/2011, Checked online:- 11/08/2013

[229] Computer Misuse Act 1990, 1990 Chapter 18
http://www.legislation.gov.uk/ukpga/1990/18/contents
Enacted:- 29/06/1990, Checked online:- 11/08/2013

[230] ICO, DPA 1998, Bring your own device (BYOD)
http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.pdf, page 6
Published:- 13/03/2013, Checked online:- 11/08/2013

[231] ICO, Data Protection, The employment practices code
http://www.ico.org.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/the_employment_practices_code.ashx,
Published:- 21/11/2011, Checked online:- 11/08/2013

[232] The European Convention on Human Rights, ROME 4 November 1950, and its Five Protocols
http://www.hri.org/docs/ECHR50.html
Checked online:- 11/08/2013

[233] Copland v The United Kingdom (2007) 45 EHRR 37, 25 BHRC 216, [2007] ECHR 253, 2 ALR Int'l 785

ECHR-C that both the Regulation of Investigatory Powers Act 2000[234] (the 2000 Act) and Telecommunications (Lawful Business Practice) Regulations 2000[235] came into force with respect domestic law after the events occurred and therefore could not be taken into consideration with respect to the case in question. The Telecommunications Regulations 2000 advises that system controllers make reasonable efforts to inform employees (Section 3(2,c)) that monitoring is taking place, however given those same regulations provide several circumstances by which lawful interception of communication is allowed (Section 3(1)), what would be considered reasonable would have to be determined by the courts, not withstanding the issues regarding compliance with both DPA 1998 and ECHR-L in such circumstances. This becomes a greater challenge with BYOD, as the device would have access to both the employee's personal data, as well as the employer's data, and distinguishing between the spheres of data ownership provides a technical and legal challenge to ensure the rights of both parties are properly respected. Organisations are advised to implement remote wipe capabilities in the event that a device is lost or stolen[236] and if organisations have not implemented a BYOD policy that specifically includes consent with respect to allowing remote wipe of personal devices, this would present a legal issue. It is likely the device contains user's personal information such as personal contacts, photographs and applications purchased by the device owner. Therefore a remote wipe instigated by the employer would be considered an invasion of privacy as per Article 8 of the ECHR-L, and also contravening Section 3 of the Computer Misuse Act[237] by impairing access to data and conversion which involves the deliberate exercise of control over chattel to the complete 'exclusion' or 'deprivation' of others[238]. Even if users accept the terms of the employers BYOD usage policy, which may include provision for remote wipe, such an action

[234] Regulation of Investigatory Powers Act 2000, 2000 Chapter 23,
http://www.legislation.gov.uk/ukpga/2000/23/contents,
Enacted:- 28/07/2000, Checked online:- 11/08/2013
[235] The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Statutory Instruments 2000 No. 2699 Investigatory Powers
http://www.legislation.gov.uk/uksi/2000/2699/contents/made
Came into force:- 24/10/2000, Checked online:- 11/08/2013
[236] Centre for the Protection of National Infrastructure, Mobile Devices, Guide for Implementers
https://www.cpni.gov.uk/Documents/Publications/Non-CPNI_pubs/2013-02-22-mobile_devices_guide_for_implementers.pdf
Published:- 27/02/2013, Checked online:- 11/08/2013
[237] Computer Misuse Act 1990, Computer misuse offences, Section 3, Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
http://www.legislation.gov.uk/ukpga/1990/18/section/3
Checked online:- 11/08/2013
[238] S. Douglas, 'The Nature of Conversion' [2009] CLJ 198, 209 – 217

should have the end users freely given consent before it is performed. If the employer relies upon a clause within a contract of employment or a BYOD policy implying consent to perform a remote wipe, where the user would be disadvantaged if they could not use their own device to fulfil their role within the organisation, the employee must have the opportunity to provide explicit consent to a remote wipe. If this is not the case, it would be considered that consent had not be freely given as the employee would not have the opportunity to withdraw such consent and therefore such an arrangement would not satisfy Article 7 or Article 8[239] of the ECHR-L. The point of implied consent was discussed within the case of DPP v. Lennon[240]where a computer owner would have considered to have given implied consent with regards to using their device for sending and receiving of email for the purposes of communication. However this consent is not unlimited, therefore excluding messages not for the purposes of communication but instead used for interrupting the proper operation and use of the computer, such as a remote wipe.

Germany's influence with respect to European legislation has been noted earlier and is considered to be more stringent with respect to protecting the rights of the employees with respect to the retention of private data belonging to those employees. The Higher Regional Court of Dresden ruled within a case[241] that businesses must retain mail databases that may contain employee personal emails, even if the employee no longer works for that business. The back ground to this case was an employee was a courier and as part of his employment he was provided an iPhone and accessories, which he used to receive both work related and personal emails into a single business email account.
Thus even though the employee used a company device and email service, the business still had a duty to protect that data belonging to the employee and not the business, until the employee has indicated they have no interest in that data, even after the employee is no longer employed by that business. The implication with BYOD is that organisations have a duty to ensure user's own

[239] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.
Adopted:- 13/07/2013, Checked online:- 21/07/2013
[240] DPP v. Lennon [2006] EWHC 1201, 170 J.P. 532, DC
[241] OLG Dresden, 4 Civil Division, decision of 5 September 2012, Case No. W 4 961/12 http://www.justiz.sachsen.de/esamosweb/documents/4W961.12.pdf
Published:- 19/10/2012, Checked online (via Google Translate):- 11/08/2013

devices are not erroneously wiped, and such a procedure must be sanctioned either by the owner of the device, or if the employer has sound legal justification to do so.

BYOD presents a challenge with respect to e-Discovery and requests pertaining to employee's personal devices that have been used to connect to their employers systems. Regarding litigation, UK legal procedures requires legal representatives to inform their clients considering court proceedings[242] to preserve any disclosable documents that would normally be deleted under business retention policies. The litigants are required under practice directions PD 31B.8[243] and PD 31B.9[244] to agree what documents will be in-scope with respect to the discovery process and format of the documents to be presented within court.

How this would apply to the systems not under the organisation's direct ownership, custody and control such as an employee's personal device? This point was raised within the case of North Shore Ventures Ltd v Anstead Holdings Inc[245], where it was determined that it may require the court to decide whether litigants had control of documents even if they did not have a legal right to the possession of such documents. Such circumstances may lead litigants to make application for third party disclosure[246], requiring employees or ex-employees to provide access to their personal equipment for the purpose of retrieving electronic documents pertinent to the case in question.

A recent court case[247]specifically covered the issue of the right of a business to access emails relating to its business specific activity held on an individual's personal computer. The arrangement was slightly different in that an agency agreement was in place between the

[242] Ministry of Justice, Practice Direction 31B – disclosure of electronic documents, Preservation of documents http://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b#IDALBUJC
Updated: - 13/06/2013, Checked online:- 11/08/2013
[243] Ibid, Discussions between the parties before the first Case Management Conference in relation to the use of technology and disclosure
[244] Ibid
[245] North Shore Ventures Ltd v Anstead Holdings Inc [2012] EWCA Civ 11
[246] The Crown Prosecution Service, Disclosure of Material to Third Parties
http://www.cps.gov.uk/legal/d_to_g/disclosure_of_third_parties/
Checked online:- 11/08/2013
[247] Transport NV v Adkins & Anor [2013] EWCA Civ 886
http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWCA/Civ/2013/886.html&query=Cadenza&method=boolean
Published:- 19/07/2013, Checked online:- 11/08/2013

business and the individual contracted to work on behalf of the business, however the court case highlighted[248]the circumstances were pertinent to employment situations as well. The business forwarded all emails to the individual and deleted or didn't retain any copies within its own ICT systems. The business submitted a claim to have a copy of all business associated emails held on the individual's own computer, which was originally denied but subsequently overturned in a court of appeal. The court of appeal came to the conclusion that the agent had a duty to provide copies of any form of documentation, inclusive of emails, relating to business activity regardless of their content, to the principle as per the agency agreement. It was of course a mistake on the behalf of the business to delete or not retain a copy of emails forwarded to the individual in the first instance; however this does not detract from their legal claim to have copies created from the individual's personal computer. The proposed use of an independent third party to perform the task of retrieval ensured the rights of the individual with respect to privacy were still retained, so that any emails relating to the individuals' private life were exclusive of the order[249]. This case highlights how BYOD presents a very real challenge to accessing business related information when not protected via measures such as DLP.

DPA 1998 allows the processing of data to meet a "legal obligation"[250], but what happens if an employee refuses to give their consent to submit their device for the purposes of responding to a Subject Authority Request (SAR)[251]? The ICO issued draft guidance is that if an organisation has made a reasonable consideration that a user's personal device may process information which falls under the SAR, access would be required to that device to retrieve such data. An employee's refusal to provide the device could mean breach of their employment contract, which

[248] Ibid paragraph 20 & paragraph 35
[249] Ibid paragraph 13
[250] ICO, DPA 1998, Legal Guidance
http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf
Published:- 30/09/2009, Checked online:- 11/08/2013
[251] ICO, Data Protection, subject access code of practice, Dealing with requests from individuals for personal information
http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF
Published:- 02/08/2013, Checked online:- 11/08/2013

once again brings into question regarding employees giving their "freely given" consent[252] the resolution of which would no doubt take longer than the 40 calendar days which organisations are obligated to respond to a SAR[253]. If the employee had copied confidential information onto their personal device or computer, for reasons other than required by their employment, the company may dismiss the employee for gross misconduct[254], however the employee may cite the Human Rights Act under Article 8 for breaching their privacy as a reason not to hand over their own device because it contains personal information. If the request for the employee to hand over their personal device is "In accordance with the law" as per paragraph 2 of ECHR-L, then such interference would be considered legitimate, a point clarified in the case of Steeg and Wenger v Germany[255]. However the request must be proportionate with regards to the reasons for the request, otherwise the employer could still risk breaching Article 8 of the ECHR-L as determined within the case Buck v Germany[256]. This stress between different pieces of legislation must be carefully considered to ensure the organisation makes a qualified judgement to determine the best course of action. This can be further complicated if legislation between different jurisdictions are in direct conflict, as in the case of Christopher X, Cour de Cassation[257], where the French Supreme Court upheld a conviction and €10,000 fine against French lawyer facilitating a discovery order under a U.S. judicial proceeding, which the French court determined was breaching the French Blocking Statute[258], and data processing laws[259].

BYOD: Too easy to mix social circles?

The rise of social networks over the past few years has been phenomenal with reports forecasting that by 2014, approximately 25% of the world wide population will be participating within an

[252] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf
Adopted:- 13/07/2013, Checked online:- 21/07/2013
[253] ICO, Subject access requests: how do I respond?
http://www.ico.org.uk/for_organisations/data_protection/subject_access_requests
Checked online:- 12/08/2013
[254] Brandeaux Advisers (UK) Ltd v Chadwick, [2010] EWHC 3241 (QB)
[255] Steeg and Wenger v Germany (2008) 47 E.H.R.R. SE16 Applications Nos 9676/05, 10744/05, 41349/06
[256] Buck v Germany (41604/98), (2006) 42 E.H.R.R. 21
[257] Christopher X, Cour de Cassation, Chambre Criminelle, Paris, December 12, 2007, No. 07-83228
[258] "French Blocking Statute" (Law No. 68-678 of 26 July 1968), as amended
[259] ACT 78-17 of 6 January 1978, on Data Processing, Data Files and Individual Liberties
http://www.ssi.ens.fr/textes/a78-17-text.html
Checked online:- 11/08/2013

online social network[260], and by 2017 the number of individuals having a social network account will be 2.55 billion. The rise in user numbers can be attributed to mobile connectivity[261]enabling and encouraging individuals to include social media as part of their everyday life[262]. The explosive growth of online social networks has not gone unnoticed by business, which has leveraged social media to interact with the public and build relationships with customers[263]. A case study of Nordic Investment Bank[264]recommended that the bank should concentrate its efforts on using LinkedIn to gain greater reach with the target audience. However the use of social networks presents challenges when employees use their own accounts to conduct communications with their employer's clients, which would not be out of the norm when using their own device. The case of Hays v Ions[265] is a clear example of where a social network provided a medium to transfer information assets, which in this case the defendant was required to disclose all his LinkedIn contacts, information which had been obtained from his employer. If the employer had implemented DLP technology the transfer of data may have been prevented in the first instance, especially with the propensity for the use of mobile applications to access social networking sites.

[260] eMarketer, Social Networking Reaches Nearly One in Four Around the World,
http://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976
Published:- 18/06/2013, Checked online:- 11/07/2013
[261] Nielsen, State of the Media, The Social Media Report 2012
http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2012-Reports/The-Social-Media-Report-2012.pdf
Published:- 05/12/2012, Checked online:- 11/07/2013
[262] Official Film website for Instragramis
http://instagramis.com/
Checked online:- 11/07/2013
[263] How does industry use social networking sites? An analysis of corporate dialogic uses of Facebook, Twitter, YouTube, and LinkedIn by industry type, Daejoong Kim, Jang-Hyun Kim and Yoonjae Nam, Quality & Quantity International Journal of Methodology © Springer Science+Business Media Dordrecht 2013 10.1007/s11135-013-9910-9
http://link.springer.com/content/pdf/10.1007%2Fs11135-013-9910-9.pdf
Published:- 28/07/2013, Checked online:- 04/08/2013
[264] Social Media in the B2B Banking & Finance Landscape, Case: Nordic Investment Bank, Dan- Roald Steinnes, http://theseus17-kk.lib.helsinki.fi/bitstream/handle/10024/55097/Social%20Media%20in%20the%20B2B%20Banking%20and%20Finance%20Landscape-%20Case%20NIB.pdf?sequence=1,
Published:- 31/01/2013, Checked online:- 11/08/2013
[265] Hays Specialist Recruitment (Holdings) Ltd v Ions [2008] EWHC 745 (Ch); [2008] I.R.L.R. 904

Conclusion

If I was to address the original question, on whether organisations have the right to implement data loss technologies on employees' device, there is no definitive yes or no answer, more a "yes, but".

Unless a variation of the existing employment contract is bilaterally agreed, organisations cannot force employees to participate in BYOD programmes, which would be a breach of Employment Rights Act 1996[266] and companies could risk constructive dismissal claims[267]as a result.

Research has shown that employees still have concerns with respect to BYOD[268], more to do with security and legal aspects rather than privacy. There is a clear need for DLP technologies, especially with regards to organisations addressing their legal liabilities and this should be clearly explained to employees, especially with respect to BYOD programmes, in order mutual respect, understanding and trust is maintained.

The ability to remotely wipe an employee's device of all its contents is a concern and I would advocate explicit consent, either from the employee or an authorised representative of the organisation, before such an action is instigated.

Even as this dissertation is being written, new business paradigms and technologies are evolving that may overcome the challenges discussed. Corporate owned personally owned (COPE[269]) programs introduces the concept where devices are supplied by the employer therefore retaining

---

[266] Employment Rights Act 1996 (c.18) s.1 & s.2(4)
http://www.legislation.gov.uk/ukpga/1996/18
Enacted:- 22/05/1996, Checked online:- 12/08/2013

[267] Norris v Great Dawley Parish Council, 04/11/2008, Employment Appeal Tribunal, EAT/0266/08

[268] Investigating the Influence of Security, Privacy and Legal Concerns on Employee's Intention to Use BYOD Mobile Devices, Benedikt Lebek, Kenan Degirmenci, Michael H. Breitner,
http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/8/
Published:- 13/05/2013, Checked online:- 12/08/2013

[269] The Guardian, Media Network, Corporate owned, personally enabled – better than bring your own device? Benjamin Robbins
http://www.theguardian.com/media-network/media-network-blog/2013/apr/24/corporate-owned-personally-enabled-cope-byod
Published:- 24/04/2013, Checked online:- 12/08/2013

complete ownership, custody and control, but employees may install personal applications etc, creating a synergy between UWYT and BYOD.

Software applications are continually advancing, and there are proposals for employee's devices to connect via virtual clients[270], isolating the device from the business infrastructure but still enabling access; but this is subject to connectivity, no signal no access.

Another promising technological solution is the use of a "Sand-box"[271], isolating organisational data on the employee's device, where DLP measures would prevent transference to employee's personal storage, thereby addressing the concerns of "Remote Wipe" deleting personal data.

Phone manufacturers are being encouraged to develop a "kill switch"[272] capability to disable a device, in the event it is stolen, lost etc. This capability would render the device inaccessible, unless re-activated with appropriate credentials, therefore in all probability the data held on the device would be protected from unauthorised access.

DLP technologies are not a panacea to resolving the question of data security[273]and their implementation presents challenges with regards to how they maybe circumnavigated[274]. Internal security threats certainly exist, but if organisations can clearly demonstrate all

[270] BYOD VMs Mini Project, School of Engineering and Computer Science Notre Dame, John Bernhard, Robert Bixler, Olivia Choudhury, Will McBurney, and Rachael Purta
http://netscale.cse.nd.edu/twiki/pub/Edu/GradOSF12MiniProjects/MiniProjectBenardPurtaEtc.pdf
Published:- 21/11/2012, Checked online:- 12/08/2013
[271] InformationWeek Mobility, MDM: To Sandbox Or Not To Sandbox? Michael A. Davis
http://www.informationweek.com/mobility/security/mdm-to-sandbox-or-not-to-sandbox/231902065
Published:- 01/11/2011, Checked online:- 12/08/2013
[272] Mail Online, Apple first to launch 'kill switch' for stolen iPhones as Boris Johnson calls for mobile phone manufacturers to do more to curb thefts, Steve Robson
http://www.dailymail.co.uk/news/article-2371391/Apple-launch-kill-switch-stolen-iPhones-Boris-Johnson-calls-mobile-phone-manufacturers-to-curb-thefts.html
Published:- 20/07/2013, Checked online:- 12/08/2013
[273] University of Mannheim, Can Data Leakage Prevention Prevent Data Leakage? Matthias Luft
http://www1.cs.fau.de/filepool/thesis/bachelorarbeit-2009-luft.pdf
Published 27/03/2009, Checked online:- 12/08/2013
[274] University of Agder, Data Loss Prevention Systems and Their Weaknesses, Tore Torsteinbø
http://www.fim.uni-linz.ac.at/Diplomarbeiten/Masterarbeit%20Tore%20Torsteinb%F8%20(2).pdf
Published 31/05/2012, Checked online:- 12/08/2013

reasonable measures have been implemented to mitigate these threats (such as DLP), while respecting the rights of their employees this will be the best possible outcome.

Bibliography

- 2011 Cost of Data Breach Study: Global, Ponemon Institute LLC, http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf, Published:- 17/07/2013, Checked online:- 06/07/2013
- ACT 78-17 of 6 January 1978, on Data Processing, Data Files and Individual Liberties http://www.ssi.ens.fr/textes/a78-17-text.html, Checked online:- 11/08/2013
- Alaka H, MHRA, List of Terminated, Revoked and Cancelled Manufacturing and Wholesale Dealer Licences 2010 - 2013 http://www.mhra.gov.uk/home/groups/is-lic/documents/publication/con062556.pdf, Last Updated 06/08/2013, Checked online:- 11/08/2013
- Analysis of Internal Data Theft, ID Analytics Inc, http://www.idanalytics.com/assets/whitepaper/IDAnalyticsInternalDataTheftWhitepaper071808.pdf, Published 28/07/2008, Checked online:- 07/07/1013
- Andrew P Moore, Dawn Cappelli, Caron, C Thomas, Eric D Shaw, Derrick Spooner, and Randall F Trzeciak, "A Preliminary Model of Insider Theft of Intellectual Property (2011)" Software Engineering Institute, Paper 726, http://repository.cmu.edu/sei/726, Published:- 06/01/2011, Checked online:- 07/07/2013
- Anne-Marie Hayden, Office of the Privacy Commissioner of Canada, News Release, WhatsApp's violation of privacy law partly resolved after investigation by data protection authorities http://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp,Published:- 28/01/2013, Checked online:- 11/08/2013
- AOL Inc, Autoblog, Press Release, Malaysian-backed Lotus F1 Racing gears up for 2010 http://www.autoblog.com/2009/10/16/malaysian-backed-lotus-f1-racing-gears-up-for-2010/, Published:- 14/10/2009, Checked online:- 11/08/2013
- Artazcoz L, Cortes I, Escriba-Aguir V, Bartoll X, Basart H, Long working hours and health status among employees in Europe: between-country differences http://www.researchgate.net/publication/233798254_Long_working_hours_and_health_status_among_employees_in_Europe_between-country_differences/file/d912f50bdef2ed6ada.pdf, Published:- 03/12/2012, Checked online:- 28/07/2013

- Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, Published:- 14/03/2013, Checked online:- 20/07/2013
- Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, Adopted:- 13/07/2013, Checked online:- 21/07/2013
- Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, Adopted:- 13/07/2013, Checked online:- 21/07/2013
- Bank of England, official website, http://www.bankofengland.co.uk/Pages/home.aspx, Checked online:- 11/08/2013
- Bank of England, Policy statement, Financial penalties imposed by the Bank http://www.bankofengland.co.uk/financialstability/Documents/fmi/penalties.pdf, Published:- 11/04/2013, Checked online:- 11/08/2013
- Bank of England, Prudential Regulation Authority, Consultation Paper CP5/13, Strengthening capital standards: implementing CRD IV http://www.bankofengland.co.uk/pra/Documents/publications/policy/2013/implementingcrdivcp513.pdf, Published:- 02/08/2013, Checked online:- 11/08/2013
- Bank of England, Prudential Regulation Authority, MAR 1.4 Market abuse (improper disclosure) http://media.fshandbook.info/content/full/MAR/1/4.pdf, Published:- 02/08/2013, Checked online:- 11/08/2013
- Bank of England, Prudential Regulation Authority, Market Conduct http://media.fshandbook.info/content/full/MAR.pdf , Published:- 02/08/2013, Checked online:- 11/08/2013
- Bank of England, Prudential Regulation Authority, official website http://www.bankofengland.co.uk/pra/Pages/about/default.aspx , Checked online:- 11/08/2013

- Banking Act 2009, 2009 Chater 1, http://www.legislation.gov.uk/ukpga/2009/1/contents, Enacted:- 12/12/2009, Checked online:- 11/08/2013
- Benedikt Lebek, Kenan Degirmenci, Michael H. Breitner, Investigating the Influence of Security, Privacy and Legal Concerns on Employee's Intention to Use BYOD Mobile Devices http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/8/, Published:- 13/05/2013, Checked online:- 12/08/2013
- Benjamin Robbins, The Guardian, Media Network, Corporate owned, personally enabled - better than bring your own device? http://www.theguardian.com/media-network/media-network-blog/2013/apr/24/corporate-owned-personally-enabled-cope-byod, Published:- 24/04/2013, Checked online:- 12/08/2013
- Bernnat,R.,O. Acker,N. Bieber, and M. Johnson, Booz & Co, Friendly Takeover - The consumerization of corporate IT (2010) http://www.booz.com/media/uploads/FriendlyTakeoverVPFINAL.pdf, Published:- 26/04/2010, Checked online:- 11/08/2013
- Bianca Bosker, The Huffington Post, Facebook Android App Collects Phone Numbers Without Permission -- Even From Non-Members http://www.huffingtonpost.com/2013/06/28/facebook-android-app-phone-numbers_n_3518652.html, Published:- 28/06/2013, Checked online:- 11/08/2013
- Bjorn Niehaves, Sebastian Koffer, Kevin Ortbach, Stefan Katschewitz, ERCIS, Towards an IT Consumerization Theory - A Theory and Practice Review http://www.ercis.org/sites/default/files/publications/2012/ercis_working_report_13_-_consumerization_0.pdf Published:- 07/2012, Checked online:- 11/08/2013
- Bjorn Niehaves, Sebastian Koffer, Kevin Ortbach, Stefan Katschewitz, ERCIS, Towards an IT Consumerization Theory - A Theory and Practice Review, http://www.ercis.org/sites/default/files/publications/2012/ercis_working_report_13_-_consumerization_0.pdf Published:- 07/2012, Checked online:- 11/08/2013
- Brandeaux Advisers (UK) Ltd v Chadwick, [2010] EWHC 3241 (QB)
- Buck v Germany (41604/98), (2006) 42 E.H.R.R. 21
- Catherine Barnard, Simon Deakin and Richard Hobbs, Opting out of the 48-hour week - Employer Necessity or Individual Choice? An Empirical Study of the operation of Article 18(1)(B) of the Working Time Directive in the UK

http://www.cbr.cam.ac.uk/pdf/wp282.pdf, Published:- 15/04/2004, Checked online:- 11/08/2013

- Centre for the Protection of National Infrastructure, Critical control 17: Data loss prevention, http://www.cpni.gov.uk/advice/cyber/Critical-controls/in-depth/critical-control17/, Checked online:- 11/08/2013
- Centre for the Protection of National Infrastructure, Mobile Devices, Guide for Implementers https://www.cpni.gov.uk/Documents/Publications/Non-CPNI_pubs/2013-02-22-mobile_devices_guide_for_implementers.pdf, Published:- 27/02/2013, Checked online:- 11/08/2013
- Christopher X, Cour de Cassation, Chambre Criminelle, Paris, December 12, 2007, No. 07-83228
- City and County of Swansea v Mr D A Gayle, Appeal No. UKEAT/0501/12/RN, 16 April 2013
- Claire Davenport, Reuters, EU to ease new data rules, http://www.reuters.com/article/2013/06/06/eu-privacy-idUSL5N0EI2Q720130606, Published:- 06/06/2013, Checked online:- 11/08/2013
- COD - Ordinary legislative procedure (ex-codecision procedure) 2012/0011(COD), http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en#tab-0, Last Updated: - 08/03/2013, Checked online:- 11/08/2013
- Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, Reference: IP/12/46 http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, Published:- 25/01/2012, Checked online:- 11/08/2013
- Commission Regulation (EU) No 611/2013, on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF, Published:- 24/06/2013, Checked online:- 21/07/2013
- Computer Misuse Act 1990, 1990 Chapter 18 http://www.legislation.gov.uk/ukpga/1990/18/contents, Enacted:- 29/06/1990, Checked online:- 11/08/2013

- Computer Misuse Act 1990, Computer misuse offences, Section 3, Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc http://www.legislation.gov.uk/ukpga/1990/18/section/3, Checked online:- 11/08/2013
- Copland v The United Kingdom (2007) 45 EHRR 37, 25 BHRC 216, [2007] ECHR 253, 2 ALR Int'l 785
- Copyright, Designs and Patents Act 1988, 988 Chapter 48 http://www.legislation.gov.uk/ukpga/1988/48/contents Enacted:- 15/11/1998, Checked online:- 11/08/2013
- Covell J, Information Commissioner's Office, The Guide to Privacy and electronic communications, section on Security of Services, http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/security_of_services, Published:- 08/09/2011, Checked online:- 11/08/2013
- Criminal Justice and Immigration Act 2008, 2008 c. 4 Part 11 Penalties for serious contraventions of data protection principles, Section 144, http://www.legislation.gov.uk/ukpga/2008/4/section/144/prospective#section-144-1, Enacted: - 8th May 2008, Checked online:- 11/08/2013
- Crowson Fabrics Limited v Paul Rider, Warren Stimson, Concept Textiles Limited [2007] EWHC 2942 (Ch)
- Daejoong Kim, Jang-Hyun Kim and Yoonjae Nam, How does industry use social networking sites? An analysis of corporate dialogic uses of Facebook, Twitter, YouTube, and LinkedIn by industry type, Quality & Quantity International Journal of Methodology © Springer Science+Business Media Dordrecht 2013 10.1007/s11135-013-9910-9 http://link.springer.com/content/pdf/10.1007%2Fs11135-013-9910-9.pdf, Published:- 28/07/2013, Checked online:- 04/08/2013
- Dan- Roald Steinnes, Social Media in the B2B Banking & Finance Landscape, Case: Nordic Investment Bank http://theseus17-kk.lib.helsinki.fi/bitstream/handle/10024/55097/Social%20Media%20in%20the%20B2B%20Banking%20and%20Finance%20Landscape-%20Case%20NIB.pdf?sequence=1, Published:- 31/01/2013, Checked online:- 11/08/2013

- Data Protection Act 1998, 1998 c. 29 Part VI Unlawful obtaining etc. of personal data Section 55, http://www.legislation.gov.uk/ukpga/1998/29/section/55, Enacted 16/071998, Checked online: -11/08/2013
- Data Protection Act 1998, 1998 CHAPTER 29 http://www.legislation.gov.uk/ukpga/1998/29/contents, Enacted 16/071998, Checked online: -11/08/2013
- Data Protection Act 1998, Schedule 1Part I Section 7 http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/paragraph/7, Checked online: -11/08/2013
- DPP v. Lennon [2006] EWHC 1201, 170 J.P. 532, DC
- Draft Communications Data Bill - Draft Communications Data Bill Joint, Conclusion, and summary of recommendations, Section 316, http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7911.htm, Published: - 11/12/ 2012, Checked online: -11/08/2013
- Draft Statutory Instrument, 2013 No. 0000, Financial Services and Markets, TheAlternative Investment Fund Managers Regulations 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/198211/aifm_regulations_090513.pdf, Published:- 09/05/2013, Checked online:- 11/08/2013
- eMarketer, Social Networking Reaches Nearly One in Four Around the World http://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976, Published:- 18/06/2013, Checked online:- 11/07/2013
- Emma Bryan, Independent police complaints commission, IPCC, independent report into loss of data relating to Child Benefit, http://www.ipcc.gov.uk/Documents/investigation_commissioner_reports/final_hmrc_report_25062008.pdf, Published: -24/06/2008, Checked online:- 11/08/2013
- Employees tell the truth about your company's data; How to make mobile devices safe for work and play, Aruba Networks http://www.arubanetworks.com/pdf/solutions/EB_mdmreport.pdf, Published:- 10/07/2013, Checked online:- 11/08/2013

- Employment Rights Act 1996 (c.18) s.1 & s.2(4) http://www.legislation.gov.uk/ukpga/1996/18, Enacted:- 22/05/1996, Checked online:- 12/08/2013
- Enterprise Act 2002, 2002 Chapter 40 http://www.legislation.gov.uk/ukpga/2002/40/contents, Enacted:- 07/11/2002, Checked online:- 11/08/2013
- EU Commission Directive 2003/94/EC http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:262:0022:0026:EN:PDF, Published:- 14/10/2003, Checked online:- 11/08/2013
- EU Commission Regulation (EU) No 611/2013, on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF, Published:- 24/06/2013, Checked online:- 11/08/2013
- EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security Published:- 07/02/2013, Checked online:- 12/08/2013
- EU Directive 2001/83/EC of the European parliament and of the Council, http://ec.europa.eu/health/files/eudralex/vol-1/dir_2001_83_cons/dir2001_83_cons_20081230_en.pdf, Published:- 30/12/2008, Checked online:- 11/08/2013
- EU DIRECTIVE 2001/83/EC of the European Parliament, Official Journal L - 311, 28/11/2004, p. 67 - 128 with subsequent amendments, http://www.edctp.org/fileadmin/documents/ethics/DIRECTIVE_200183EC_OF_THE_EUROPEAN_PARLIAMENT.pdf, Published:- 10/09/2004, Checked online:- 11/08/2013
- EC Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0051:EN:PDF

Published:- 24/04/2002, Checked online:- 12/08/2013

- EC Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF Published:- 31/07/2002, Checked online:- 12/08/2013
- EU Directive 2003/6/EC, insider dealing and market manipulation (market abuse) http://www.esma.europa.eu/system/files/Dir_03_6.pdf, Published:- 12/04/2003, Checked online:- 11/08/2013
- EU Directive 2003/88/EC concerning certain aspects of the organisation of working time http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:299:0009:0019:EN:PDF, Published:- 18/11/2003, Checked online:- 11/08/2013
- EU Directive 2009/136/EC of the European Parliament and of the Council, Official Journal of the European Union, L 337/11 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF, Published:- 18/12/2009, Checked online:- 11/08/2013
- EU Directive 2009/E/EC on the legal protection of computer programs http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF, Published:- 05/05/2009, Checked online:- 11/08/2013
- EU Directive 2011/61/EU, on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:174:0001:0073:EN:PDF, Published:- 01/07/2011, Checked online:- 11/08/2013
- EU Directive 2011/62/EU of the European Parliament and of the Council http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:174:0074:0087:EN:PDF, Published:- 01/07/2011, Checked online:- 11/08/2013
- EU Directive 96/9/EC, on the legal protection of databases http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1996:077:0020:0028:EN:PDF, Published:- 27/03/1996, Checked online:- 11/08/2013

- EudraLex - Volume 4 Good manufacturing practice (GMP) Guidelines http://ec.europa.eu/health/documents/eudralex/vol-4/,Published:- 04/02/2011, Checked online:- 11/08/2013
- European Commission, Explanatory Memorandum for the proposed new legal framework General Data Protection Regulation http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, Published:- 25/01/2012, Checked online:- 11/08/2013
- European Commission, The EU Single Market, Capital Requirements Directive: Legislation in force http://ec.europa.eu/internal_market/bank/regcapital/legislation_in_force_en.htm, Published:- 17/07/2013, Checked online:- 11/08/2013
- European Data Protection Supervisor, Additional EDPS comments on the Data Protection Reform Package, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf, Published:- 15/03/2013, Checked online:- 11/08/2013
- European Federation of Pharmaceutical Industries and Associations, The Pharmaceutical Industry in Figures, Key Data 2012 http://www.efpia.eu/uploads/Modules/Documents/efpia_figures_2012_final-20120622-003-en-v1.pdf, Published:- 15/06/2012, Checked online:- 11/08/2013
- European Parliament News, EU Bank Capital Requirements Regulation and Directive, REF: 20130412BKG07195 http://www.europarl.europa.eu/news/en/pressroom/content/20130412BKG07195/html/EU-Bank-Capital-Requirements-Regulation-and-Directive, Published:- 15/04/2013, Checked online:- 11/08/2013
- European Securities and Markets Authority (ESMA), Official website http://www.esma.europa.eu, Checked online:- 11/08/2013
- Explanatory Memorandum for the proposed new legal framework General Data Protection Regulation http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, Published:- 25/01/2012, Checked online:- 11/08/2013

- Explanatory Memorandum to The Privacy And Electronic Communications (EC Directive) (Amendment) Regulations 2011, 2011 No. 1208 http://www.legislation.gov.uk/uksi/2011/1208/pdfs/uksiem_20111208_en.pdf, Published:- 05/05/2011, Checked online:- 11/08/2013
- Exploring ways to Model Reputational Loss, Cas de Bie, http://www.jbisa.nl/download/?id=8762035, Checked online: - 06/07/2013
- Facebook, official website https://www.facebook.com/ , Checked online:- 11/08/2013
- FDA, FD&C Act Chapter III: Prohibited Acts and Penalties http://www.fda.gov/regulatoryinformation/legislation/federalfooddrugandcosmeticactfdcact/fdcactchapteriiiprohibitedactsandpenalties/default.htm, Last Updated:- 08/06/2012, Checked online:- 11/08/2013
- FDA, Federal Food, Drug, and Cosmetic Act (FD&C Act) http://www.fda.gov/regulatoryinformation/legislation/federalfooddrugandcosmeticactfdcact/default.htm, Last Updated:- 05/12/2011, Checked online:- 11/08/2013
- FDA, Inspections, Compliance, Enforcement, and Criminal Investigations, Mediagnost GmbH 08/05/2012 http://www.fda.gov/iceci/enforcementactions/warningletters/2012/ucm308110.htm, Last Updated:- 13/06/2012, Checked online:- 11/08/2013
- FDA, Medical Devices, Code of Federal Regulations - Title 21 http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.10, Last Updated:- 01/04/2013, Checked online:- 11/08/2013
- FDA, Vaccines, Blood & Biologics, Notice of Intent to Revoke (NOIR) Letter: Allergy Laboratories, Inc http://www.fda.gov/biologicsbloodvaccines/guidancecomplianceregulatoryinformation/complianceactivities/administrativeactionsbiologics/ucm344480.htm Last Updated:- 20/03/2013, Checked online:- 11/08/20
- Federal Constitutional Court, 1BvR 370/07, 27.2.2008, paragraph no. (1 - 333) http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, Published:- 27/02/2008, Checked online:- 11/08/2013
- Final Report, ESMA's technical advice to the European Commission on possible implementing measures of the Alternative Investment Fund Managers Directive, Ref:

ESMA/2011/379 http://www.esma.europa.eu/system/files/2011_379.pdf, Published:- 16/11/2011, Checked online:- 11/08/2013

- Financial Conduct Authority Handbook, Recognised Investment Exchanges, REC 2.3.6, Operational and other risks http://fshandbook.info/FS/html/FCA/REC/2/3, Published:- 01/04/2013, Checked online:- 11/08/2013
- Financial Conduct Authority, "Make a regulatory announcement" http://www.fca.org.uk/firms/markets/ukla/information-dissemination/announcement, Published:- 31/03/2013, Checked online:- 11/08/2013
- Financial Conduct Authority, Disclosure Rules and Transparency Rules (DTR), Legitimate interests and when delay will not mislead the public http://fshandbook.info/FS/html/FCA/DTR/2/5#D126, Last Updated:- 01/04/2013, Checked online:- 11/08/2013
- Financial Conduct Authority, Disclosure Rules and Transparency Rules (DTR), Requirement to disclose inside information http://fshandbook.info/FS/html/FCA/DTR/2/2, Published:- 01/04/2013, Checked online:- 11/08/2013
- Financial Conduct Authority, official website, www.fca.org.uk, Checked online:- 11/08/2013
- Financial Conduct Authority, Recognised Investment Exchanges https://www.fsa.gov.uk/register/exchanges.do, Last Updated:- 11/08/2013 Checked online:- 11/08/2013
- Financial Services Act 2010, 2010 Chapter 28, http://www.legislation.gov.uk/ukpga/2010/28/contents, Enacted:- 08/14/2010, Checked online:- 11/08/2013
- Financial Services Act 2012, 2012 Chapter 21, http://www.legislation.gov.uk/ukpga/2012/21/contents/enacted, Enacted:- 19/12/2012, Checked online:- 11/08/2013
- Financial Services and Markets Act 2000, 2000 Chapter 8, http://www.legislation.gov.uk/ukpga/2000/8/contents, Enacted:- 14/07/2000, Checked online:- 11/08/2013

- Financial Services and Markets Act 2000, Part VIII Market abuse, Section 118 (Market Abuse) http://www.legislation.gov.uk/ukpga/2000/8/section/118, Last Updated:- 31/12/2011, Checked online:- 11/08/2013
- Financial Services and Markets Act 2000, Part VIII Market abuse, Section 118B (Insiders) http://www.legislation.gov.uk/ukpga/2000/8/section/118B, Last Updated:- 01/07/2005, Checked online:- 11/08/2013
- Financial Services and Markets Act 2000, Part XVIII, Recognised Investment Exchanges and Clearing Houses http://www.legislation.gov.uk/ukpga/2000/8/part/XVIII, Checked online:- 11/08/2013
- Financial Services Authority, Data Security in Financial Services http://www.fsa.gov.uk/pubs/other/data_security.pdf, Published:- 23/08/2008, Checked online:- 11/08/2013
- Fitzgerald International v Tradition (UK) Ltd [2000] R.P.C. 95; [1999] Masons C.L.R. 157
- Force India Formula One Team Ltd v 1 Malaysia Racing Team Sdn Bhd [2012] EWHC 616 (Ch); [2012] R.P.C. 29;
- Frank La Rue, United Nations, General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, Published:- 15/04/2008, Checked online:- 11/08/2013
- French Blocking Statute (Law No. 68-678 of 26 July 1968), as amended
- Gartner Press Release, Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes http://www.gartner.com/newsroom/id/2466615, Published:- 01/05/2012, Checked online:- 11/08/201
- Gerrit Hornung & Christoph Schnabel, Computer Law & Security Report, Volume 25, Issue 1, 2009, Pages 84-88, Data protection in Germany I: The population census decision and the right to informational self-determination http://cms.uni-kassel.de/unicms/fileadmin/groups/w_030405/Ehemalige_Mitarbeiter/Dr._Christoph_Schnabel/Hornung___Schnabel__Data_protection_in_Germany_I__CLSR_2009__84.pdf, Published:- 2009, Checked online:- 11/08/2013

- Guideline on Management of Computerized Systems for Marketing Authorization Holders and Manufacturers of Drugs and Quasi-drugs, (entative translation not formally authorized by Ministry of Health, Labour and Welfare of Japan) http://www.pmda.go.jp/english/service/pdf/gmp/guideline_for_computerized_systems/20110817.pdf, Published:- 17/08/2011, Checked online:- 11/08/2013
- Hays Specialist Recruitment (Holdings) Ltd v Ions [2008] EWHC 745 (Ch); [2008] I.R.L.R. 904
- HM Treasury, Creating stronger and safer banks http://www.hm-treasury.gov.uk/fin_financial_services_bill.htm, Last Updated:- 17/07/2013, Checked online:- 11/08/2013
- HM Treasury, official website, https://www.gov.uk/government/organisations/hm-treasury, Last Updated:- 09/08/2013, Checked online:- 11/08/2013
- Home Office, Covert Surveillance and Property Interference, Revised Code of Practice https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, Published:- 17/03/2010, Checked online:- 11/08/2013
- House of Commons Justice Committee, The functions, powers and resources of the Information Commissioner, Ninth Report of Session 2012-13, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/962/962.pdf, Published:- 12/03/2013, Checked online:- 21/07/13
- House of Commons, Hansard Debates., 21 January 2008, c1225 http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080121/debtext/80121-0006.htm#0801215000512, Checked online:- 11/08/2013
- House of Commons, Select Committee on Justice, First Report, Problems with data protection http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/15402.htm, Published: - 17/12/2007, Checked online:- 11/08/2013
- House of Lords, Constitution Committee - Second Report, Surveillance: Citizens and the State http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm, Published:- 21/01/2009, Checked online:- 11/08/2013
- House of Lords, Constitution Committee - Second Report, Surveillance: Citizens and the State, Chapter 8: the role of Citizens

http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1810.htm, Published:- 21/01/2009, Checked online:- 11/08/2013

- Information Commissioner's guidance about the issue of monetary penalties prepared and issued under Section 55C (1) of the Data Protection Act 1998, ISBN: 9780108511240, http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.ashx, Published 2012, Checked online:- 11/08/2013
- Information Commissioner's Office, DPA 1998, Bring your own device (BYOD) http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.pdf, Published:- 13/03/2013, Checked online:- 11/08/2013
- Information Commissioner's Office, Case Reference Number: ENF0379519, Undertaking by Co-operative Life Planning Ltd, http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/co-op_life_planning_undertaking.ashx, Checked online:- 11/08/2013
- Information Commissioner's Office, Data Protection Act 1998, What is personal data? - A quick reference guide, http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf, Published: -18/04/2008, Checked online:- 11/08/2013
- Information Commissioner's Office, Data Protection, subject access code of practice, Dealing with requests from individuals for personal information http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF, Published:- 02/08/2013, Checked online:- 11/08/2013
- Information Commissioner's Office, Data Protection, The employment practices code http://www.ico.org.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/the_employment_practices_code.ashx, Published:- 21/11/2011, Checked online:- 11/08/2013
- Information Commissioner's Office, DPA 1998, Legal Guidance http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guid

es/data_protection_act_legal_guidance.pdf, Published:- 30/09/2009, Checked online:- 11/08/2013

- Information Commissioner's Office, Enforcing the revised Privacy and Electronic Communications Regulations (PECR), http://www.ico.org.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/enforcing_the_revised_privacy_and_electronic_communication_regulations_v1.pdf, Published:- 25/05/2011, Checked online:- 11/08/2013
- Information Commissioner's Office, Monetary Penalty Notice [PECR], Mr Christopher Anthony Niebel trading as Tetrus Telecoms http://www.ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Notices/tetrus_niebel_monetary_penalty_notice.ashx, Published:- 26/11/2012, Checked online:- 11/08/2013
- Information Commissioner's Office, Monetary Penalty Notice [PECR], Mr Gary John Peter McHeish trading as Tetrus Telecoms http://www.ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Notices/tetrus_mcneish_monetary_penalty_notice.ashx, Published:- 26/11/2012, Checked online:- 11/08/2013
- Information Commissioner's Office, Press Release, Co-operative Life Planning commits to take action after thousands of customers' details were made available online http://www.ico.org.uk/~/media/documents/pressreleases/2011/coop_news_release_20110526.ashx, Published:- 26/05/2008, Checked online:- 11/08/2013
- Information Commissioner's Office, Press Release, Spam texters fined nearly half a million pounds as ICO cracks down on illegal marketing industry, http://www.ico.org.uk/news/latest_news/2012/spam-texters-fined-nearly-half-a-million-pounds-28112012, Published:- 28/12/2012, Checked online:- 11/08/201
- Information Commissioner's Office, Privacy by design, http://www.ico.org.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf, Published:- 11/2008, Checked online:- 11/08/2013
- Information Commissioner's Office, Subject access requests: how do I respond? http://www.ico.org.uk/for_organisations/data_protection/subject_access_requests, Checked online:- 12/08/2013

- Intellectual Property Office, Copyright Rights in Performances Publication Right, Database Right. Unofficial consolidated text of UK Legislation to 3 May 2007 http://www.ipo.gov.uk/cdpact1988.pdf , Published:- 15/09/2011, Checked online:- 11/08/2013
- Intellectual Property Office, official website http://www.ipo.gov.uk/ , Checked online:- 11/08/2013
- International Organization for Standardization, official website http://www.iso.org/iso/home.html Checked online:- 11/08/2013
- Jan Lauren Boyles, Aaron Smith and Mary Madden, Privacy and Data Management on Mobile Devices http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf, Published:- 05/09/2012, Checked online:- 20/07/2013
- Jan Philipp Albrecht, Draft Report on General Data Protection Regulation, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/924/924343/924343en.pdf, Published:- 16/01/2013, Checked online:- 11/08/2013
- John Bernhard, Robert Bixler, Olivia Choudhury, Will McBurney, and Rachael Purta, BYOD VMs Mini Project, School of Engineering and Computer Science Notre Dame http://netscale.cse.nd.edu/twiki/pub/Edu/GradOSF12MiniProjects/MiniProjectBenardPurtaEtc.pdf, Published:- 21/11/2012, Checked online:- 12/08/2013
- Joseph Menn, Special Report: U.S. cyberwar strategy stokes fear of blowback http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510, Published:- 10/05/2013, Checked online:- 28/07/2013
- Leo Kelion, BBC News, Q&A: NSA's Prism internet surveillance scheme http://www.bbc.co.uk/news/technology-23051248, Published:- 01/07/2013, Checked online:- 11/08/2013
- Lise M. Saaria and Timothy A. Judge, Employee Attitudes and Job Satisfaction, Human Resource Management, Winter 2004, Vol 43, No 4, Pages 395-407 http://utm.edu/staff/mikem/documents/jobsatisfaction.pdf, Published:- 02/12/2004, Checked online:- 20/07/2013
- London Economics, Implications of the European Commission's proposal for a general data protection regulation for business,

http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Research_and_reports/implications-european-commissions-proposal-general-data-protection-regulation-for-business.ashx, Published:- 14/05/2012, Checked online:- 11/08/2013

- London Stock Exchange, Official website http://www.londonstockexchange.com/, Checked online:- 11/08/2013
- MacCartney v Oversley House Management, Employment Tribunal, 31 January 2006 [2006] I.C.R. 510; [2006] I.R.L.R. 514
- Marshall Andria, OnePoll Survey, UK Insider Threat - consumer, http://logrhythm.com/Portals/0/resources/LogRhythm_survey_results_4.2013_employees.pdf, Published:- 10/05/2013, Checked online:- 07/07/2013
- MasterCard Worldwide, MasterCard Rules http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf, Published:- 14/07/2013, Checked online:- 11/08/2013
- Matthias Luft, University of Mannheim, Can Data Leakage Prevention Prevent Data Leakage? http://www1.cs.fau.de/filepool/thesis/bachelorarbeit-2009-luft.pdf, Published 27/03/2009, Checked online:- 12/08/2013
- Medicines Act 1968, 1968 CHAPTER 67, http://www.legislation.gov.uk/ukpga/1968/67, Enacted 25/10/1968, Checked online:- 11/08/2013
- MHRA, Manufacturer's and wholesale dealer's licences, http://www.mhra.gov.uk/Howweregulate/Medicines/Licensingofmedicines/Manufacturersandwholesaledealerslicences/index.htm, Last Updated 06/08/2013, Checked online:- 11/08/2013
- MHRA, Registration of Brokers introduced by the Falsified Medicines Directive 2011/62/EU http://www.mhra.gov.uk/home/groups/es-policy/documents/websiteresources/con224464.doc, Published:- 25/03/2008, Checked online:- 11/08/2013
- MHRA, Review of EU medicines legislation - proposals for implementation, http://www.mhra.gov.uk/home/groups/comms-ic/documents/websiteresources/con007679.pdf, Published:- 21/03/2005, Checked online:- 11/08/2013

- Michael A. Davis, InformationWeek Mobility, MDM: To Sandbox Or Not To Sandbox? http://www.informationweek.com/mobility/security/mdm-to-sandbox-or-not-to-sandbox/231902065, Published:- 01/11/2011, Checked online:- 12/08/2013
- Ministry of Justice, Practice Direction 31B - disclosure of electronic documents, Preservation of documents http://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b#IDALBUJC Updated: - 13/06/2013, Checked online:- 11/08/2013
- Morgan Marquis-Boire, Bill Marczak and Claudio Guarnieri, The SmartPhone Who Loved Me: FinFisher Goes Mobile? https://citizenlab.org/wp-content/uploads/2012/08/11-2012-thesmartphonewholovedme.pdf, Published:- 08/2012, Checked online:- 28/07/2013
- Ms Niharika, B.Y.O.D. Genie Is Out Of the Bottle - "Devil Or Angel", Journal of Business Management & Social Sciences Research (JBM&SSR) ISSN No 2319-5614 Volume 1, No. 3, http://www.borjournals.com/Research_papers/Dec_2012/1060%20%20M.pdf, Published:- 14/12/2012, Checked online:- 11/08/2013
- National Archive of Financial Services Authority website http://webarchive.nationalarchives.gov.uk/*/http:/www.fsa.gov.uk/, Last Updated:- 26/06/2013, Checked online:- 11/08/2013
- Nielsen, State of the Media, The Social Media Report 2012 http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2012-Reports/The-Social-Media-Report-2012.pdf, Published:- 05/12/2012, Checked online:- 11/07/2013
- Norris v Great Dawley Parish Council, 04/11/2008, Employment Appeal Tribunal, EAT/0266/08
- North Shore Ventures Ltd v Anstead Holdings Inc [2012] EWCA Civ 11
- Official Film website for Instragramis http://instagramis.com/, Checked online:- 11/07/2013
- Official website for the Pharmaceuticals and Medical Devices Agency, Japan (English text) http://www.pmda.go.jp/english/index.html, Checked online:- 11/08/2013

- OLG Dresden, 4 Civil Division, decision of 5 September 2012, Case No. W 4 961/12 http://www.justiz.sachsen.de/esamosweb/documents/4W961.12.pdf, Published:- 19/10/2012, Checked online (via Google Translate):- 11/08/2013
- Paul A. Pavlou, Huigan Liang, Yajion Xue, Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal Agent Perspective, MIS Quarterly Vol 31 No 1 Pages 105-136 http://im1.im.tku.edu.tw/~myday/teaching/992/SEC/S/992SEC_T5_Paper_20100415_UNDERSTANDING%20AND%20MITIGATING%20UNCERTAINTY%20IN%20ONLINE%20EXCHANGE%20RELATIONSHIPS.pdf, Published:- 03/2007, Checked online:- 11/08/2013
- Payment Card Industry (PCI), Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf, Published:- 29/08/2011, Checked online:- 11/08/2013
- PCI Security Standards Council, LLC, official website https://www.pcisecuritystandards.org/, Checked online:- 11/08/2013
- Pinsent Masons artice, City sackings and suspensions at a five-year high http://www.out-law.com/en/articles/2013/january/city-sackings-and-suspensions-at-a-five-year-high/, Published:- 14/01/2013, Checked online:- 11/08/2013
- Ponemon Institute LLC, The Risk Of Insider Fraud, Second Annual Study, http://www.unfaircompetitiontradesecretscounsel.com/PonemonInstituteTheRiskOfInsiderFraud.pdf Published:- 02/2013, Checked online:- 06/07/2013
- PR Newswire US, BYOD Gives Competitive Advantage, Say IT Managers. http://www.prnewswire.com/news-releases/byod-gives-competitive-advantage-say-it-managers-151687995.html Published:- 16/05/2012, Checked online:- 17/07/2013
- Practical Law, Market abuse: FSA decision notice for improper disclosure http://uk.practicallaw.com/0-518-7926?q=email+insider+information#null, Published:- 03/04/2012, Checked online:- 11/08/2013
- Proposal for an EU Directive on Network and Information Security- ICO consultation response, http://www.ico.org.uk/about_us/consultations/~/media/documents/consultation_response

s/response-to-eu-directive-on-network-and-information-security-call-for-evidence-responses-to-consultations-and-inquiries.pdf, Published:- 04/07/2013, Checked online:- 21/07/2013

- Protection of Freedoms Act 2012, 2012 Chapter 9, http://www.legislation.gov.uk/ukpga/2012/9/enacted, Enacted:- 01/05/2012, Checked online:- 11/08/2013
- PwC, Bring your own device, Agility through consistent delivery http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/byod-1-25-2012.pdf, Published:- 25/01/2012, Checked online:- 11/08/2013
- Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:364:0001:0001:EN:PDF Published:- 09/12/2004, Checked online:- 12/08/2013
- Regulation of Investigatory Powers Act 2000, 2000 Chapter 23, http://www.legislation.gov.uk/ukpga/2000/23/contents, Enacted:- 28/07/2000, Checked online:- 11/08/2013
- Regulation of Investigatory Powers Act 2000, Part II Authorisation of surveillance and human intelligence sources, Section 32, Authorisation of intrusive surveillance http://www.legislation.gov.uk/ukpga/2000/23/section/32, Checked online:- 11/08/2013
- Reputational Contagion and Optimal Regulatory Forbearance, http://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1196.pdf, Published:- May 2010, Checked online:- 06/07/2013
- Rich Mogull, Understanding and Selecting a Data Loss Prevention Solution, https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf, Published:- 04/12/2007, Checked online:- 30/06/2013
- S. Douglas, 'The Nature of Conversion' [2009] CLJ 198, 209 - 217
- Sarah Ludford, Liberal Democrat MEP, EU Data Protection, dialogue on draft Regulation, http://www.sarahludfordmep.org.uk/node/2238, Published:- 29/05/2013, Checked online:- 11/08/2013
- SAS Institute Inc. v World Programming Ltd [2013] EWHC 69 (Ch) - 25/01/13

- Scott Reeves, Make sure BYOD doesn't mean Bring Your Own Disaster http://www.techrepublic.com/blog/data-center/make-sure-byod-doesnt-mean-bring-your-own-disaster/, Published:- 15/02/2013, Checked online:- 28/07/2013
- Shakespeare review of public sector information, Department for Business, Innovation & Skills, https://www.gov.uk/government/publications/shakespeare-review-of-public-sector-information, Published:- 15/05/2013, Checked Online:- 21/07/2013
- Spencer H. Silverglate and Craig Salner, Smartphones and the Fair Labor Standards Act http://cspalaw.com/pdf/Smartphones.pdf, Published:- 01/06/2011, Checked online:- 11/08/2013
- Staff Fraud Scape. Depicting the UK's fraud landscape, CIFAS https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Staff_Fraudscape_CIFAS_webversion.pdf,Published:- 03/04/2013, Checked online:- 06/07/2013
- Steeg and Wenger v Germany (2008) 47 E.H.R.R. SE16 Applications Nos 9676/05, 10744/05, 41349/06
- Stephen Moss, The Guardian Book Blog, George Orwell back in fashion as Prism stokes paranoia about Big Brother http://www.guardian.co.uk/books/booksblog/2013/jun/11/george-orwell-prism-big-brother-1984, Published:- 11/06/2013, Checked online:- 11/08/2013
- Steve Robson, Mail Online, Apple first to launch 'kill switch' for stolen iPhones as Boris Johnson calls for mobile phone manufacturers to do more to curb thefts http://www.dailymail.co.uk/news/article-2371391/Apple-launch-kill-switch-stolen-iPhones-Boris-Johnson-calls-mobile-phone-manufacturers-to-curb-thefts.html, Published:- 20/07/2013, Checked online:- 12/08/2013
- Symantec Corporation, What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk, https://www4.symantec.com/mktginfo/whitepaper/WP_WhatsYoursIsMine-HowEmployeesarePuttingYourIntellectualPropertyatRisk_dai211501_cta69167.pdf, Published:- 01/02/2013, Checked online:- 07/07/2013
- Tejaswini Heratch and H. Raghav Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations, European Journal of

Information Systems (2009) 18, pages 106-125, http://www.som.buffalo.edu/isinterface/papers/ejis20096.pdf, Published:- 27/05/2009, Checked online:- 20/07/2013

- Telegraph Article, 'Doing a Ratner' and other famous gaffes, http://www.telegraph.co.uk/news/uknews/1573380/Doing-a-Ratner-and-other-famous-gaffes.html, Published 22/12/2007, Checked online:- 07/07/13
- The British Standards Institution, official website http://www.bsigroup.co.uk, Checked online:- 11/08/2013
- The Copyright and Rights in Databases Regulations 1997, PART II Regulation 6 http://www.legislation.gov.uk/uksi/1997/3032/regulation/6/made Checked online:- 11/08/2013
- The Copyright and Rights in Databases Regulations 1997, Statutory Instruments 1997 No. 3032 http://www.legislation.gov.uk/uksi/1997/3032/contents/made, Came into force:- 01/01/1998, Checked online:- 11/08/2013
- The Crown Prosecution Service, Disclosure of Material to Third Parties http://www.cps.gov.uk/legal/d_to_g/disclosure_of_third_parties/, Checked online:- 11/08/2013
- The Data Protection (Monetary Penalties) Order 2010, Statutory Instruments, 2010 No. 910 http://www.legislation.gov.uk/uksi/2010/910/introduction/made, Came into force:- 06/04/2010, Checked online:- 11/08/13
- The European Convention on Human Rights, ROME 4 November 1950, and its Five Protocols http://www.hri.org/docs/ECHR50.html, Checked online:- 11/08/2013
- The failure of Northern Rock: A Multi-dimensional Case Study ISBN-13: 978-3-902109-46-0, Page 19 http://www.suerf.org/download/studies/study20091.pdf, Published:- 2009, Checked online:- 07/07/13
- The Government Response to Shakespeare Review of Public Sector Information, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207600/Government_Response_to_Shakespeare_Review_of_Public_Sector_Information.pdf, Published:- June 2013, Checked online:-20/07/2013

- The Human Medicines Regulations 2012, PART 1 The licensing authority and the Ministers, Regulation 6, http://www.legislation.gov.uk/uksi/2012/1916/regulation/6/made Came into force:- 14/08/2012, Checked online:- 11/08/2013
- The Human Medicines Regulations 2012, Statutory Instruments 2012 No. 1916, Medicines http://www.legislation.gov.uk/uksi/2012/1916/contents/made, Came into force:- 14/08/2012, Checked online:- 11/08/2013
- The Literature Network, George Orwell, 1984, Summary Part 1, Chapter 1 http://www.online-literature.com/orwell/1984/2/, Checked online:- 11/08/2013
- The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, Statutory Instruments 2011 No. 1208, Electronic Communications http://www.legislation.gov.uk/uksi/2011/1208/contents/made, Came into Force:- 20/05/2011, Checked online:- 11/08/2013
- The Privacy and Electronic Communications (EC Directive) Regulations 2003, Statutory Instruments, 2003 No. 2426, http://www.legislation.gov.uk/uksi/2003/2426/contents/made, Came into force:- 11/12/2010, Checked online:- 11/08/13
- The Right Honourable Lord Justice Leveson, An Inquiry Into The Culture, Practices And Ethics Of The Press Executive Summary, http://www.official-documents.gov.uk/document/hc1213/hc07/0779/0779.pdf, Published:- 11/2012, Checked online:- 21/07/2013
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Statutory Instruments 2000 No. 2699 Investigatory Powers http://www.legislation.gov.uk/uksi/2000/2699/contents/made, Came into force:- 24/10/2000, Checked online:- 11/08/2013
- The Working Time Regulations 1998, PART II Regulation 4, Maximum weekly working time http://www.legislation.gov.uk/uksi/1998/1833/regulation/4/made, Checked online:- 11/08/2013
- The Working Time Regulations 1998, PART IV Regulation 35, Restrictions on contracting out http://www.legislation.gov.uk/uksi/1998/1833/regulation/35/made, Checked online:- 11/08/2013

- The Working Time Regulations 1998, Statutory Instrument 1998 No. 1833 http://www.legislation.gov.uk/uksi/1998/1833/contents/made, Came into force:- 01/10/1998, Checked online:- 11/08/2013
- TNS Infratest, Kaspersky Lab PR Survey 2013 - Netherlands http://newsroom.kaspersky.eu/fileadmin/user_upload/nl/Campaign/KESB2013/Misc/Report_NL_Kaspersky_Lab_2013.pdf, Published:- 15/03/2013, Checked online:- 11/08/2013
- Tore Torsteinbø, University of Agder, Data Loss Prevention Systems and Their Weaknesseshttp://www.fim.uni-linz.ac.at/Diplomarbeiten/Masterarbeit%20Tore%20Torsteinb%F8%20(2).pdf, Published 31/05/2012, Checked online:- 12/08/2013
- Transport NV v Adkins & Anor [2013] EWCA Civ 886 http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWCA/Civ/2013/886.html&query=Cadenza&method=boolean, Published:- 19/07/2013, Checked online:- 11/08/2013
- United States National Security Agency, Official Website http://www.nsa.gov/, Checked online:- 11/08/2013
- University of Bristol Information Security Policy http://www.bristol.ac.uk/infosec/policies/docs/isp-18.pdf, Published:- 08/01/2013, Checked online:- 11/08/2013
- VISA, If Compromised http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html, Checked online:- 11/08/2013
- Viviane Reding, Women and the Web - Why Data Protection and Diversity belong together, http://europa.eu/rapid/press-release_SPEECH-13-637_en.htm, Published:- 15/07/2013, Checked online:- 11/08/2013
- WhatsApp Inc official website http://www.whatsapp.com/, Checked online:- 11/08/2013