

Newsletter

January 2013

Contents

Sony fined £250,000 following hacking attack

[Page 1](#)

ICO discusses EU data protection reforms

[Page 2](#)

Bank employee fined for unlawfully obtaining bank statements

[Page 3](#)

Information Commissioner's response to the Leveson Report

[Page 4](#)

ICO consults on subject access code of practice

[Page 5](#)

ICO comments on the draft Communications Data Bill

[Page 5](#)

ICO highlights concerns over protection of personal data in local government

[Page 6](#)

ICO highlights FOI requests made in 2012

[Page 8](#)

ICO announces freedom of information monitoring of four public authorities

[Page 8](#)

International Focus - Dubai

[Page 9](#)

SCL Seminar - Have you got IT covered

[Page 9](#)

Contributors

[Page 10](#)

Sony fined £250,000 following hacking attack

Sony operated the PlayStation network platform, and was the data controller in respect of the personal data provided by customers when they created an account to access the network platform. The network platform, including customer databases, was administered and maintained on Sony's behalf by a US service provider (which was part of the Sony group). The network platform was used by millions of customers in Europe, the Middle East, Africa, Australia and New Zealand. The network platform was infiltrated following hacking attacks on various online networks of the Sony group. The attacker accessed personal data stored on the network platform, including millions of customers' names, addresses, email addresses, dates of birth and account passwords. The incident was voluntarily reported by Sony to the ICO.

The Commissioner [held](#) that there had been a serious breach of the data protection principle that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". Sony failed to ensure that appropriate technical measures were taken, such as additional cryptographic controls to protect passwords and updating the relevant software. Sony had been subject to hacking attacks prior to this attack, and should have therefore anticipated a further attack and taken appropriate security measures. The Sony group is part of a multinational group of companies with sufficient resources to address security issues. The breach was likely to cause substantial damage or distress to the affected accountholders, and Sony was therefore fined £250,000.



ICO discusses EU data protection reforms

The ICO has published a [blog post](#) on EU data protection reforms. The ICO suggests that the planned reforms could amount to one of the biggest changes to the data protection regime that the UK has ever experienced. The ICO is heavily involved in the UK's input on the reforms and states that it is playing close attention to developments in the legislative process.

The initial reform proposals were published by the European Commission in January 2012. The next step in the legislative process involves the European Parliament and the Council of the European Union looking at the proposals separately, before coming together to approve a final text.

There are five committees of the European Parliament appointed to examine the proposed data protection reforms. Each committee is required to submit its own amendments before negotiating a consolidated European Parliament view on the reforms, which is expected in late April.

Running alongside this process, the Council itself is looking at the proposed reforms. The Council is made up of relevant ministers and government officials from each Member State. The Ministry of Justice represents the UK in respect of the proposed data protection reforms. It works closely with the Home Office and is being advised by the ICO.

The ICO describes how the parliamentary committees are well advanced in their scrutiny, but the Council is further behind. However, more meetings of the Council are being scheduled to ensure that the negotiations can be completed as quickly as possible, to try to keep the process on track.

Once both the European Parliament and the Council have their consolidated views, they will need to negotiate with one another, possibly over the summer, to seek agreement on the text of the legislation. Failing agreement, there will need to be another reading of the texts by the European Parliament and the Council, followed by further negotiations. According to the ICO, there is an imperative to have a package adopted by 2014, when the European Parliament and the European Commission are due for re-appointment.

In relation to the content of the discussions that are ongoing, there is a debate about whether the reforms should be in the form of a regulation (which will apply directly in every Member State) or a directive (which will need to be transposed into each Member State's national law). The current proposal is for a general regulation which will have direct effect in each Member State and a directive specifically for the criminal justice sector. According to the ICO, there is speculation that the directive will be put on the back burner. There is also a move to confine the regulation to the private sector and develop a new directive to cover the public sector, which the ICO and other data protection authorities are resisting.



Bank employee fined for unlawfully obtaining bank statements

An employee (**D**) of Barclays unlawfully accessed bank statements of her partner's ex-wife. At the time, D's partner was involved in a legal dispute over the terms of the divorce settlement with his ex-wife. According to the ICO's announcement, when certain eBay transactions were raised in a meeting between the estranged couple, the ex-wife became suspicious that her account had been viewed. Barclays were contacted and, when they began investigating, D left her job. D pleaded guilty to unlawfully obtaining personal data, which is a criminal offence under section 55 of the Data Protection Act 1998 (**DPA**). D was fined £500 by the Derby Crown Court, and ordered to pay a £15 victim surcharge and £1,410.80 prosecution costs.

The Information Commissioner commented that he felt the level of the fine was inadequate and that there is a need for more effective sentences (which the ICO believes should include prison sentences) to deter the unlawful access and use of personal information. The ICO's statement on the case can be found [here](#).

Information Commissioner's response to the Leveson Report

The Information Commissioner has published his response to the Leveson Report, which can be found [here](#). The Leveson Report sets out proposals designed to improve the culture, practices and ethics of the press, and includes comments on and recommendations for the ICO and the DPA.

The Information Commissioner acknowledges that the Leveson Report is critical of the work of the ICO relating to the regulation of the press. However, he points out that since the period during which the bulk of the activity analysed by the Leveson Inquiry took place (2003-2007) the ICO has changed a lot, with the ICO having an enhanced enforcement tool kit and a more effective management structure.

In response to the Leveson Report's specific recommendations for the ICO, the Information Commissioner has proposed, among other things, the following action points:

- Revising the ICO's Data Protection Regulatory Action Policy to include details on how the ICO will use its regulatory powers in relation to the press
- In consultation with the press and broadcasting industry and the new press regulator, developing a Code of Practice on the DPA and the media
- Preparing and issuing guidance to the public on their individual rights in relation to the obtaining and use of their personal data by the press, and how to exercise those rights
- Adding a section to the ICO's website dedicated to giving advice to individuals on their information rights vis-à-vis the media
- Drafting a stakeholder engagement plan detailing the key stakeholders in the press and the nature and frequency of contact required. Once completed, considering establishing a media reference panel, to ensure a ready source of expertise is available to the ICO on key media issues
- Continuing to digest the Leveson Report and considering whether the ICO should establish a cross-office Enforcement Board to oversee the application of all the ICO's prosecution and civil enforcement powers

The Information Commissioner also provided his views on certain recommendations of the Leveson Report directed at the Ministry of Justice, including those regarding:

- Scaling back the exemption from the obligations to comply with certain data protection principles and individual information rights, currently contained in section 32 of the DPA, in relation to the publication of journalistic material
- Allowing compensation for pure distress (not just distress associated with damage) for breach of the DPA.
- Increasing the severity of the sentences available for criminal offences under section 55 of the DPA (concerning the unlawful use of personal data)
- Increasing the scope of the prosecution powers of the Information Commissioner
- Reconstituting the ICO as an Information Commission, led by a Board of Commissioners with a suitable range of expertise

The recommendations of the Leveson Report covered in the Information Commissioner's response would, if implemented, clearly have a major impact on the ICO and the DPA. In the Information Commissioner's [blog post](#) accompanying his response to the Leveson Report, he points out that he anticipates "many long and arduous telephone conferences as the new regulatory landscape takes shape in 2013".

ICO consults on subject access code of practice

The DPA provides individuals with the right of access to their personal information held by organisations, by making a subject access request. Once received, an organisation normally has 40 days to respond to the request.

The ICO has announced a consultation on a new draft code of practice on subject access requests, to help organisations handle subject access requests while supporting the public in taking control of their personal information. According to the ICO, during the last financial year the ICO received nearly 6,000 complaints from individuals regarding subject access requests, which was more than any other type of complaint. The new code of practice will aim to explain clearly and simply an organisation's legal responsibilities and individual's rights under the DPA.

The draft code of practice and consultation document can be found [here](#). The ICO is requesting individuals and organisations that have experience in handling or making subject access requests to review the draft code and provide their opinions. The closing date for the consultation is 21 February 2013, and the final code will be published in spring 2013. Clyde & Co will be submitting their comments on the consultation and will publish a summarised form of these once the consultation period has closed. If you have any comments which you would like to be fed in to the consultation, please do let your usual Clyde & Co contact know, or email Isabel Ost (isabel.ost@clydeco.com).

ICO comments on the draft Communications Data Bill

The draft Communications Data Bill proposes, among other things, to expand the powers of certain public authorities (in particular law enforcement authorities) to obtain "communications data" from "telecommunications operators", requiring them to log data of internet activity for the purpose of countering crime committed online. These powers will require additional data collection and retention by telecommunications operators. The new powers will be subject to certain safeguards, including as to data security and integrity and the destruction of data. Under the current draft, the ICO would be responsible for policing these safeguards.

The Joint Committee of both Houses of Parliament recently published a report on the Bill, which can be found [here](#). The ICO has published a statement responding to this report, which is available [here](#).

The Information Commissioner stated that he is concerned about the adequacy of the proposed safeguards that the ICO will be responsible for regulating. In addition, to ensure the security of retained personal information and its destruction after a certain period of time, the ICO believes it will require increased powers and resources. The

Information Commissioner was therefore pleased to see this issue referred to in the report of the Joint Committee. The Information Commissioner emphasised (in a theme that seems to run through much of this month's news) that the report added to calls for stronger deterrent sentences for those misusing personal information, which the Information Commissioner calls to be implemented without delay.

The draft Communications Data Bill is currently being redrafted.



ICO highlights concerns over protection of personal data in local government

The ICO has highlighted its concerns relating to the standard of data protection in local government, following its recent issuance of a number of monetary penalties against local councils. The ICO has criticised local governments' attitudes towards protecting personal data. The Information Commissioner stated that recent fines have been caused by councils "treating sensitive personal data in the same routine way they would deal with more general correspondence" and that councils are often not appearing to have "acknowledged that the data they are handling is about real people, and often the more vulnerable members of society". The recent penalties mean that 19 local councils have now received monetary penalties for breaching the DPA, totalling £1,885,000. The ICO states that it is pressing the Ministry of Justice for stronger powers to audit local councils', as well as NHS bodies', data protection compliance, if necessary without consent.

The facts of some of the recent decisions are summarised below:

Leeds City Council: A support assistant in the children services department re-used (in line with the Council's policy) an envelope, which was originally intended for an unrelated external third party, for internal mail, but forgot to cross out the original address. The envelope was delivered to the originally-marked external recipient. The enclosed documents contained personal data relating to four data subjects, including confidential and highly sensitive personal data relating to a young person (including details of a criminal offence). Although the Council had overarching policies relating to data protection and information security, which were available to staff on its intranet together with limited training, there were no specific policies or training on security measures to be applied when sending sensitive personal data to internal or external third parties. The unintended recipient (a grandmother who had previously received correspondence from the Council relating to one of her grandchildren) sent an email to inform the Council that she received the documents. The Council collected the documents and sent a letter of apology to the affected individuals.

Devon County Council: A social worker prepared an adoption panel report using another family's report as a template, to remind her of the type of information to be included. The social worker was asked to send additional copies of her report to its original recipients, but accidentally sent copies of the template family's report. The template family's report contained confidential and highly sensitive personal data relating to approximately 22 data subjects, including information on the ethnic origin, religion, mental and physical health and alleged criminal activities of a couple being considered as part of the adoption process. The recipients did not return the template family's report for over two months. The Council had overarching policies on data protection and personal information security, but could not demonstrate that the social worker had read the policies and there was no specific guidance on the handling or posting of sensitive information. Data protection training, although available, was not mandatory and the social worker had not undertaken any of the Council's information governance training packages.

London Borough of Lewisham: A social worker on his probationary period took case papers relating to a child protection matter out of the office so that he could prepare for an upcoming court hearing over the weekend. Social workers were allowed by the Borough to take case papers out of the office without permission. The papers were carried in an opaque shopping bag, which the social worker mistakenly left on the train on his journey home. The bag containing the papers was recovered from the train company's lost property office seven days later. The papers contained confidential and highly sensitive personal data relating to a family who were the subject of care proceedings due to allegations of abuse and neglect against the perpetrators, including sexual abuse. Although the Borough had overarching policies on data protection and information security, there was no specific guidance on how sensitive personal data should be transported. Although training materials were available on the intranet, the social worker had not completed the relevant training.

In each of these cases, the Information Commissioner held that there was a serious breach of the data protection principle that "[a]ppropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". In each case, the breach was considered likely to cause substantial distress to the affected data subjects.

Each of the councils failed to take appropriate organisational measures against unauthorised processing/accidental loss of personal data. The appropriate measures differed in each case and included:

- Having different envelopes for internal and external mail that are clearly distinguishable
- Having a peer checking process for envelopes containing confidential and sensitive personal data
- Having appropriate and robust policies, guidelines, procedures and training for staff
- Providing security locks for bags and considering a more secure means of accessing sensitive personal data out of the office (e.g. encrypted USB pens)

Leeds City Council was [fined £95,000](#), Devon County Council was [fined £90,000](#) and the London Borough of Lewisham was [fined £70,000](#).

ICO highlights FOI requests made in 2012

The ICO has published a [news release](#) illustrating the kind of information that has successfully been obtained during 2012 by way of freedom of information requests made under the Freedom of Information Act 2000. Under the Act, individuals have the right to ask public authorities for official documents (eg minutes of council meetings and details of public spending). The public authority must then provide the information or explain why the information should not be disclosed. Individuals can complain to the ICO if a public authority wrongly refuses to release the requested information.

According to the news release, Ministry of Justice figures showed that 37,313 information requests were made to central government offices in the first three quarters of 2012, with many more being made to local councils, NHS bodies, police forces and other public authorities. Freedom of information requests revealed, for example, that there are 43,586,400 fake one pound coins in circulation and the amount of gifts given to the Metropolitan Police Force by businesses.

Looking forward, the Deputy Information Commissioner describes how he expects more information to become available in 2013. Changes to the regime are being explored to look at the way public authorities release information, which could include providing data in formats that make it easier to process and analyse and providing licences for others to re-use information to benefit the public.

ICO announces freedom of information monitoring of four public authorities

The ICO has [announced](#) that the Department for Education, the Department for Work and Pensions, the Office of the First Minister and Deputy First Minister in Northern Ireland and Wirral Metropolitan Borough Council will be monitored for the first quarter of 2013 over concerns about the timeliness of their responses to freedom of information requests. These public authorities were selected for monitoring as they either failed to respond to 85% of freedom information requests within the time limit of 20 working days or had exceeded the time limit by a significant margin on numerous occasions. The Information Commissioner stated that the ICO may take further action after the monitoring period has expired if there is not the necessary improvement in the authorities' standard of compliance.



International Focus - Dubai

The DIFC Data Protection Law Amendment Law was enacted on 23 December 2012, with the intention of increased transparency, efficiency and effectiveness in the exercise of the DIFC Commissioner of Data Protection's (the Commissioner's) powers. It amends the existing DIFC Data Protection Law and the Data Protection Regulations. The Dubai International Financial Centre (DIFC) is a federal free zone in Dubai, UAE. It is one of very few jurisdictions in the Middle East to have implemented a specific data protection regime.

The key changes to the Law and Regulations are:

- A new requirement for Data Controllers to notify the Commissioner of any changes to their data processing activities within 14 days of the change(s) occurring
- An express provision that a Data Controller may contravene the Law by any act or omission that is not compliant with the Law or the Regulations
- An ability for the Commissioner to apply to the DIFC Court for an order directing compliance and the payment of costs by Data Controllers
- A formal system under which the Commissioner may impose a fine (with fines ranging from USD 5,000 to USD 25,000 depending on the relevant contravention)
- A change to the definition of Personal Data to cover

personally identifiable data processed by automatic means or recorded as part of any filing system where specific information relating to a particular individual is readily accessible

The amendments are not extensive but help to clarify Data Controllers' practical obligations under the Law. Further, the introduction of a formal system of fines is likely to assist in encouraging increased understanding of and compliance with the Law.

Please [click here](#) to view the full update

SCL Seminar – Have you got IT covered?

On 29 January 2013 Clyde & Co hosted and sponsored an IT event for the Society for Computers and Law. This seminar entitled 'Have you got IT covered?' was attended by many in-house and private practice lawyers, and representatives of insurers.

The session was chaired by Dr David Sharp of Charteris plc and the panel included [Andrew Horrocks](#), partner in Clyde & Co's Professional and Commercial Disputes team who has wide IT-related claims experience, and Phil Mayes of Lockton's Global Technology practice. The talk looked at insurance contracts and policy coverage within the IT sector, assessing IT risks and liabilities when taking out insurance, and the effect of insurance on limitation of liability clauses

in IT contracts. The seminar also covered likely future developments in this developing area of insurance including cyber-liability, BYOD (bring your own device) and cloud computing plus other legal pitfalls and issues.

For further information on any of the issues discussed, please contact Andrew Horrocks (andrew.horrocks@clydeco.com).

For more details about SCL please visit www.scl.org

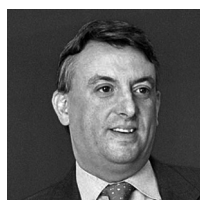


Contributors

If you would like further information on any of the issues raised in this newsletter please contact your usual Clyde & Co contact or one of the contributors to this newsletter listed below:



Alan Meneghetti
Partner, London
T: +44 (0)20 7876 5616
E: alan.meneghetti@clydeco.com



Andrew Horrocks
Partner, London
T: +44 (0)20 7876 6511
E: andrew.horrocks@clydeco.com



James Cassidy
Senior Associate, London
T: +44 (0)20 7876 6081
E: james.cassidy@clydeco.com



Isabel Ost
Associate, London
T: +44 (0)20 7876 5313
E: isabel.ost@clydeco.com



Fiona Tyas
Legal Director, Middle East
T: +971 4 384 4516
E: fiona.tyas@clydeco.com



Takamasa Makita
Legal Director, Middle East
T: +971 4 384 4673
E: takamasa.makita@clydeco.com

Clyde & Co offers international coverage on data protection and is well placed to provide an immediate response to data breaches and cyber threats wherever they occur. Our experienced data protection and privacy team spans our global network of offices across Europe, the Americas, Asia-Pacific and the Middle East - advising on a wide range of data protection and privacy issues.

Clyde & Co LLP
The St Botolph Building
138 Houndsditch
London EC3A 7AR
T: +44 (0)20 7876 5000
F: +44 (0)20 7876 5111

Further advice should be taken before relying on the contents of this summary.

Clyde & Co LLP accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary.

No part of this summary may be used, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, reading or otherwise without the prior permission of Clyde & Co LLP.

Clyde & Co LLP is a limited liability partnership registered in England and Wales. Authorised and regulated by the Solicitors Regulation Authority.
© Clyde & Co LLP 2013

Clyde & Co LLP

www.clydeco.com