

Global Privacy & Compliance Update
A Periodic Publication from
Iron Mountain's Privacy & Compliance Group
March 2011

- **France: Companies violating the Data Protection Act to be publicly named and shamed**

France's National Assembly has proposed two changes to the Data Protection Act that would 1) authorize the Data Protection Authority, the CNIL, to publish its enforcement actions, and 2) if an organization objects to an on-site inspection, the CNIL will be required obtain a court order prior to conducting the inspection. In certain circumstances, an unannounced inspection or "dawn raid" may be carried out without a court order. For further details, click on the following link: <http://www.huntonprivacyblog.com/2011/01/articles/european-union-1/french-national-assembly-votes-on-amendments-to-data-protection-act/index.html>

- **Global Bribery and Corruption Enforcement Highlights**

- 1) The Securities and Exchange Commission has charged Tyson Foods Inc. with violating the U. S. Foreign Corrupt Practices Act (FCPA) by making illicit payments to two Mexican government veterinarians who were responsible for certifying its Mexican subsidiary's chicken products for export sales. The SEC news release can be accessed at: <http://www.sec.gov/news/press/2011/2011-42.htm>
- 2) Two former directors and a sales manager of the engineering firm Mabey & Johnson Ltd have been sentenced to prison for providing kickbacks to the Iraqi government by inflating the contract price for the supply of steel bridges and disguising illegal payments that were channelled through Jordanian banks. Charles Forsyth received 21 months imprisonment, David Mabey eight months imprisonment, and Richard Gledhill eight months imprisonment. The UK Serious Fraud Office news release can be accessed at: <http://www.sfo.gov.uk/press-room/latest-press-releases/press-releases-2011/mabey--johnson-ltd-former-executives-jailed-for-helping-finance-saddam-hussein-s-government.aspx>
- 3) The UK Serious Fraud Office (SFO) announced that M.W. Kellogg Limited (MWKL), will pay over £7 million in recognition of sums it is due to receive that resulted from the criminal activity of third parties. The agreement also ensures that MWKL will overhaul its internal audit and control measures so that its compliance systems are in accordance with UK law. MWKL has also agreed to pay the costs of the investigation. The SFO news release can be accessed at: <http://www.sfo.gov.uk/press-room/latest-press-releases/press-releases-2011/mw-kellogg-ltd-to-pay-£7-million-in-sfo-high-court-action.aspx>
- 4) Philips Electronics disclosed last week in its 2010 annual report that three ex-Philips employees are being investigated for possible criminal activity involving potential violations of the U.S. Foreign Corrupt Practices Act (FCPA). This action follows an indictment by the Polish authorities of several people including the 3 former Philips employees. <http://www.reuters.com/article/2011/02/22/philips-idUSLDE71L17D20110222>

- **Massachusetts General Hospital settles loss of HIPAA data for \$1 Million and enters into a comprehensive Corrective Action Plan (CAP).**

A Mass General employee, while commuting to work, left documents on a subway train. The documents included a patient schedule containing names and medical record numbers of 192 patients, and billing forms containing the name, date of birth, medical record number, health insurer, policy number, diagnosis and name of providers for 66 of those patients. The documents were never recovered. The Department of Health and Human Services (HHS) opened its investigation into Mass General after a complaint was filed by a patient. HHS's investigation indicated that Mass General failed to implement reasonable and appropriate safeguards to protect the privacy of Protected Health Information (PHI) when removed from Mass General's premises, and impermissibly disclosed PHI potentially violating provisions of the HIPAA Privacy Rule. The settlement and the Corrective Action Plan documents can be accessed at: <http://www.hhs.gov/ocr/privacy/hipaa/news/mghnews.html>

- **How to reduce fraud**

An Article on CFO.com lists a number of steps to take and tools to use to reduce fraud such as: establishing a "hotline", conducting surprise audits, implementing anti-fraud training, implementing a Code of Conduct, implementing an Anti-fraud Policy, and conducting employee background checks. The full article can be accessed at: <http://www.cfo.com/printable/article.cfm/14557373>

- **Oracle Seeks to bar evidence in whistleblower Case**

In attempt to shield the company from liability to other potential plaintiff's, Oracle is asking a Virginia Judge to bar evidence in a \$1 Billion whistleblower suit against the company. The case, brought under the False Claims Act (FCA), alleges that from 1998 to 2006 Oracle induced the General Services Administration (GSA) to buy \$1.08 Billion in software by falsely representing that the government was receiving the same discounts as "most-favored" commercial customers when in fact it was not. Rather, Oracle passed discounts of as much as 92 percent through to other customers while the government discount ranged from 25 to 40 percent. To read more, please click here: <http://www.bloomberg.com/news/2011-02-18/oracle-seeks-to-bar-u-s-from-giving-states-whistleblower-data.html>

- **Poland's Data Privacy Law conveys new powers and obligations**

The below amendments to Poland's Data Privacy law come into force this month,

- 1) The Inspector General for the Protection of Personal Data now will be able to impose fines of about \$350 on a natural person and about \$1,700 to a company for violations. The fines are limited to a total of \$1,700 for a natural person and \$70,000 for a company
- 2) Data controllers are now required to respond to a subject access request within 30 days, and to provide the full details of all processing
- 3) Sensitive data now has to be notified/registered prior to processing
- 4) Criminal penalties of a fine or imprisonment up to 2 years are now in force for any person who prevents the Inspector General from performing an inspection activity
- 5) The definition of consent has been changed such that individuals will be able to withdraw consent at any time.

A more detailed article can be accessed at:

<http://mail.twobirds.com/ve/ZZLjiV62M81Lo59O79/VT=0/page=7#page=1>

- **In a Healthcare Privacy Violation Clinic fined \$4.3 million**

For the first time since it went into effect in 2003, U.S. federal officials have imposed a civil penalty for violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. The U.S. Department of Health and Human Services (HHS) charged Cignet Health with failing to provide 41 patients a copy of their requested medical records within the 60 day privacy rule window under HIPAA. \$3 million of the fine was for willful neglect because Cignet was uncooperative during the investigation and refused to provide the medical records even when issued a federal subpoena. After a court order, Cignet finally produced the documents for the 41 patients but also delivered an additional 4,500 records of other patients that were not part of the investigation. To read more on this topic, please click here: <http://www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html>, here: <http://thehill.com/blogs/healthwatch/other/145533-health-insurer-fined-43m-for-hipaa-violation>, and here: <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207094.html>

- **EMC pays \$87.5 million in settlement of alleged kickbacks and misrepresented pricing practices under their GSA Schedule**

In a suit filed under the False Claims Act, EMC settled with the United States Government for \$87.5 Million for alleged kickbacks and misrepresenting pricing practices during negotiations with the General Services Administration. The Department of Justice said that "Misrepresentations during contract negotiations and the payment of kickbacks or illegal inducements undermine the integrity of the government procurement process.... The Justice Department is acting to ensure that government purchasers of commercial products can be assured that they are getting the prices they are entitled to." To read more click here: <http://thehill.com/blogs/hillicon-valley/technology/99779-emc-settles-federal-kickback-lawsuit-for-875-million>

- **Codes of Ethics are becoming more important in Russia**

While Codes of Ethics are common in large western companies operating in Russia, implementing them poses challenges. Russia ranks high on Transparency International's Corruption Perceptions Index, and government bribes or "thanks you's", as they're known locally, are seen as part of business as usual. Despite their robust Codes of Ethics, companies such as HP, Siemens, and others have paid substantial fines related to violations in their Russian offices. Read more in this recent article from The Moscow Times:

<http://www.themoscowtimes.com/business/article/business-ethics-get-codified/431517.html>

- **Techniques and tools for testing Anti-corruption and Anti-bribery Programs**

An article in Financer Worldwide notes that: "Multinational companies face regulatory imperatives to test the effectiveness of their anticorruption compliance program.... Best practices build on a company's risk assessment to identify high-risk areas, follow with data analytics to identify patterns and anomalies, and incorporate a sampling of random transactions to test for documentation shortcomings and/or employees' ability to evade controls.... Testing is best performed by a combination of internal auditors and experienced forensic accountants with a deep background in identifying corrupt activities. Substantive testing not only permits management, independent directors and significant investors to evaluate a company's investment in anti-corruption compliance measures, but also *reinforces* those elements and further demonstrates management's commitment." The full article can be accessed at:

<http://www.bdoneewswire.com/docs/Worldwatch-Fraud-and-Regulatory-Enforcement-Feb2011.pdf>