Lessons Learned from the Facebook Audits

By Rob Corbet, Partner, Arthur Cox

On 21 September 2012, the Data Protection Commissioner (“DPC”) published his second audit report on Facebook Ireland following on from the initial detailed audit report that was published in December 2011. Given Ireland’s positioning as a hub for data centers and “big data” operator, the integrity and credibility of the reports was important. In this regard, while opinions will differ in relation to the pros and cons of the audit report recommendations, the DPC’s office is to be commended in producing two comprehensive reports in what must have been trying circumstances.

The audits have encouraged Facebook to adopt a more transparent approach to their data management practices. For example, a more prominent privacy policy has been agreed and more transparency has been introduced to disclose the fact of third party access to data using social plug-ins, especially in the case of any “friends” apps which grant access to personal data without a person’s knowledge.

The DPC determined Facebook members should be entitled to prevent their image being tagged, notwithstanding the potential loss of control and prior notification that may come with that choice. Interestingly, this appears to have been an issue where the DPC felt that Facebook had gone further than was strictly necessary under Irish law. The Second Report notes that the feature has been removed to assuage the concerns of supervisory authorities in other jurisdictions.

The DPC has insisted upon “fully verified” account deletion at the end of the customer life cycle. In addition, Facebook has been required to improve the information provided to users in relation to what happens to deleted or removed content.

Judging by the audit reports, the proposed introduction of “Privacy by Design” under the new EU Data Protection Regulation is here already.

In keeping with the overarching principle of “fair processing”, the DPC has also convinced Facebook to provide users with more information so as to enable them to make more informed choices “inline” or “just in time” before any use of their data commences. The adoption of a “welcome dashboard” with enhanced privacy settings will also empower users to adjust their settings to suit their specific preferences at any time.
Portugal Enacts New Interoperability Rules for the Public Sector

By João Luís Traça, Partner, Miranda Correia Amendoeira & Associados

A sprawling, multi-layered public sector is the sort of administrative nightmare faced by many countries, not least of which Portugal. Over the last few years, central and local government bodies have purchased or licensed IT solutions that are ill-designed for data sharing on a public sector-wide level.

In a bid to standardize these solutions, the Portuguese Parliament enacted Law No. 36/2011, of 21 July 2011, requiring all deployments, licenses, and updates of IT systems to be subject to a set of open standards, which would be set at a later date by the Portuguese Council of Ministers.

Having finally reached a consensus on what these standards should be, the Council of Ministers issued Resolution No. 91/2012, of 8 November 2012. This statutory instrument lists a number of rules for government bodies to observe so as to ensure what is referred to as ‘digital interoperability’ of data and information. Among these rules are the aforementioned open standards for IT systems on matters running the gamut from audio/video streaming to e-mail and network security to document formats. The Resolution casts its net far and wide to make certain that no public procurement procedure for IT services or products is left out. Most of the standards included – both mandatory and recommended – borrow from documents published by the World Wide Web Consortium and The Internet Engineering Task Force.

Software, hardware, and solutions providers should carry out a thorough check to make sure that they meet these standards, or else they will likely find themselves unable to compete in public procurement procedures for which they would otherwise be eligible. Criticism may be leveled at the manifest preference for sector-wide uniformity in that it comes at the expense of innovation and restricts experimentation with multiple solutions at the same time as a means of finding the best possible one. Nevertheless, we should take care not to forget that the purpose of this measure is to guarantee the interoperability of all public sector systems.

With standardization comes greater efficiency and cost-reduction, both of which are strong reasons indeed for adopting standards already used worldwide.

Trust and Verify: Automation of Compliance with Stricter Privacy and Data Security Requirements through Cyberstructure

By Kenneth N. Rashbaum, Principal, Rashbaum Associates, LLC & Paul Watry, Ph.D., Professor at the University of Liverpool

The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information.

Viviane Redding, European Commission Vice-President and European Union Justice Commissioner, January 25, 2012 on the proposed revision of the European Union Privacy Directives (emphasis supplied).

As technological innovation facilitates the spread of e-commerce on a global scale, governments are sounding the alarm about privacy and data security protections. The European Commission’s proposal to revise the European Union Privacy Directives, if adopted, will create additional compliance requirements for global businesses and academic institutions, and significantly increase the penalties for noncompliance. This, in turn, will require multinational companies to adopt enhanced compliance monitoring, but how will they be able to afford additional personnel and equipment to meet the requirements?
monitoring standards as the worldwide global economic slowdown continues?

Automation of cross-border information transfer compliance requirements through platforms such as Integrated Rule-Oriented Data Systems (“iRODS”) may hold an answer. The iRODS data grid framework, sponsored in part by the National Archives and Records Administration, is instrumented to invoke automatically policies associated with specific data manipulation operations; that is, the compliance policies are “built into” the data. Examples are the automatic invocation of a policy before ingestion of a file (typically for access authorization checks), or automatic invocation after ingestion of a file (such as protocols for legally mandated safeguards of personal information when the data are disclosed). 3

iRODS transforms these policies into computer-actionable rules needed to manage data collections that will aggregate hundreds of petabytes of data (such as genomic information used for research and various therapies) and, as needed, transfer them across borders. This platform makes it possible to automate administrative functions (such as disclosure, distribution, retention, replication, synchronization), and enforce management policies such as generation of audit trails to govern and monitor access and disclosure.

Technological innovation has resulted in stricter requirements for electronic communication. Compliance personnel can meet these enhanced requirements with an innovation of their own automation.

Endnotes:

ABA SIL on the Proposed EU Data Protection Regulation

The ABA’s Section of International Law together with the Section of Antitrust (Sections) submit their comments on the EU’s Proposal for a General Data Protection Regulation.

The comments highlight the necessity for the expansion of Binding Corporate Rules for cloud processors. The Sections also emphasize that the current 24 hour reporting limit for data breaches (to authorities) should be lengthened.

The full text of the comments can be found at:
http://www.americanbar.org/content/dam/aba/administrative/international_law/joint_sil_comments_to_draft_eu_privacy_regulation.authcheckdam.pdf
French Government to Introduce Digital “Habeas Corpus” Bill in 2013

By Marie-Andrée Weiss, Attorney, Law Office of Marie-Andrée Weiss

The European Commission, which is the European Union’s (E.U.) executive body, published on January 25, 2012, a Proposal for a Regulation on the protection of individuals with regard to the processing of personal data.

As of today, the E.U. data protection rules are mainly contained in the 1995 European Union Data Protection Directive, Directive 95/46/EC. Directives are set to harmonize policy among the twenty-seven Member States, but they are not directly applicable, and merely express a set of goals and principles. Member States implement Directives in their own legal systems by enacting national laws incorporating Directives’ goals and principles.

A regulation, however, is directly applicable to all Member States. The Regulation would repeal the 1995 Directive, and therefore, there would be one E.U. data protection law for all the Member States. Or would it?

In France, the government has the power to present bills to the Parliament, and Fleur Pellerin, the minister in charge of digital economy, stated in front of the French Parliament on October 17, 2012 that she would like the Parliament to pass a new law protecting personal data and privacy on the Internet. The Minister of Justice and the French Data Protection Authority, the CNIL, will be allied in developing the bill. The government bill will be presented to the Parliament as early as the first quarter of 2013, that is, before the Regulation will finally come into effect, probably in 2014.

Such a law would be, according to Fleur Pellerin, a digital “Habeas Corpus.” This digital “Habeas Corpus” was an electoral promise of successful French Presidential candidate François Hollande, and would shield individuals from risks to their digital persona associated with new technologies.

However, if other Member States would chose to enact similar new laws, one wonders if the Regulation, once enacted, will be effectively the one and only E.U. data protection law. Fleur Pellerin did not evoke how the new law would cohabit with the Regulation, or if the bill will take inspiration from the current Regulation draft.

Source: http://www.assemblee-nationale.fr/14/cr-eco/12-13/c1213010.asp (in French)

Spreadex Limited v. Colin Cochrane [2012] EWCH 1290 (Comm)

By Rob Corbet, Partner, Arthur Cox and Claire O’Brien, Trainee Solicitor, Arthur Cox

In May 2011, the Defendant’s account on an online spread betting service incurred a loss of £50,000. It transpired that the five year old son of the defendant’s girlfriend had accessed the account and had placed the unsuccessful bets. The Claimant initiated proceedings on the contention that the defendant had no arguable grounds to defend the action. As the proceedings were for summary judgment, the Claimant could not argue that the Defendant had fabricated his version of events in order to release himself from the liability to pay after a losing streak.

Spreadex relied upon a Clause of its Customer Agreement, which stated that all trading under a user’s account number would be deemed by Spreadex to have been conducted by that user. However, the Court held that, as there was no element of consideration being provided in the Customer Agreement, it was not a legally binding contract, therefore this clause could not be enforced. Furthermore, as the Customer Agreement placed no obligations upon Spreadex and no rights were attributed to the customer,
Clause 10(3) was buried. The Court submitted the far-reaching proposition that a company is seeking to rely on its customers’ acceptance of complex terms is ‘irrational’; and that such acceptance is an entirely inadequate method of affixing liability on users.

There is a risk, that if an obligation is imposed on businesses to ‘dumb down’ terms, then important tenets of the agreement will be lost and an imbalance of rights and obligations was created which is fatal to a term of a consumer contract under Regulation 5(1) of the UTCCR.

Possibly the most significant implication of this judgment is its damning view on lengthy terms and conditions. The Judge held that it would have been a ‘miracle’ if Mr. Cochrane had read through 49 pages of ‘closely printed and complex paragraphs’ in which the onerous unforeseen consequences will occur. While a duty to highlight the most ‘important’ clauses should be encouraged as best practice, it can be a self-defeating exercise. On what basis should a business subjectively decide which clauses need to be highlighted the most? Surely every clause of a contract is intended to be valid and binding; otherwise, to have incorporated it into the contract at all would have been a pointless exercise.

Commercial Emails to Canadian Residents Now Have Guidelines for Consent Requirements for New Anti-Spam Law

By Megan Brister, Senior Manager, Deloitte and Katerina Kouretas, Associate, Gowling Lafleur Henderson LLP

The Canadian Radio-television and Telecommunications Commission (“CRTC”) published two information bulletins to help Canadian and foreign businesses better understand Canada’s anti-spam legislation (“CASL”). The bulletins clarify CASL and encourage businesses to start implementing changes now – despite the delay in CASL’s enforcement (expected in 2013). In absence of anti-spam legislation in Canada, several businesses have followed the US’ CAN-SPAM Act, which allows businesses to send emails to recipients until recipients opt out. CASL will require businesses (including organizations outside of Canada) that send commercial electronic messages (“CEM”) (e.g. email, text, Tweet, LinkedIn message) to Canadian recipients to gain the recipients’ consent. Non-compliance will carry stiff monetary penalties: up to $10 M for organizations per violation.

The CRTC provides useful details on means and methods to obtain consent in its bulletins. It is clear that express consent must be an opt-in mechanism. A toggling mechanism that pre-checks a consent box will not be sufficient. A CEM cannot be used to elicit express consent, either. It would, however, be sufficient to require the individual to actively check a blank consent box, or type in an email address to indicate consent, with a confirmation of receipt to be provided to the individual.

The CRTC’s guidelines make it clear that consent cannot be subsumed in website terms and conditions - it must be clearly identified and separate from the consent to general terms and conditions of use or sale.

Since most businesses currently use their general online terms and conditions or terms of use agreements to elicit deemed consent to receive commercial electronic messages from their customers, the CRTC will require significant changes by those businesses going forward.

The CRTC has also provided some detail on the unsubscribe mechanism to be included in a CEM. This mechanism must be “readily performed”; for emails, a link that takes the user to a webpage where the user can unsubscribe from receiving all or some types of CEM’s from the sender works, as does a reply to an SMS message with the word “STOP” or “Unsubscribe”, then clicking on a link to unsubscribe.
Privacy, E-Commerce & Data Security Committee

Co-Chairs:
Rob Corbet
Anjli Garg Pero

Vice-Chairs:
Tony Burke, Claudia Cantarella,
Adam Kardash,
Kenneth N Rashbaum,
Jose A Santos Jr,
W Gregory Voss

Newsletter Editor:
Katherine Woodcock

Upcoming Events & Webinars

BLT Live Webinar on International Data Governance and Legal Issues in New Data-Related Service Models. PEDS Vice-Chair W. Gregory Voss will be one of the panelists, discussing the proposed EU General Data Protection Regulation.

- Tuesday, December 18th at 1pm (EST).

The ABA SIL will be accepting program proposals for the Section’s 2013 Fall Meeting, which will take place from October 15-19, 2013, at the London Hilton on Park Lane in London, United Kingdom. The deadline for submissions is January 7, 2013.

For more information about the submission process, please see the proposal instructions document from the 2013 Fall Meeting Co-Chairs, available at http://ww5.aievolution.com/aba1302/files/content/docs/Fall2013ProgramProposalGuidelines.pdf

Program proposals may only be submitted online using the following form: http://ww5.aievolution.com/aba1302.

Committee News

Demetrios Eleftheriou, Senior Advisor and former Co-Chair of the PEDS Committee, has been appointed by Bart Legum, Chair of the ABA Section of International Law, to be SIL’s representative on the ABA Cybersecurity Legal Task Force. This is a great honor for Demetrios as well as the PEDS Committee.

W. Gregory Voss, Professor at Toulouse Business School and Vice-Chair of the PEDS Committee, publishes on the Proposed EU General Data Protection Regulation in the ABA’s Business Law Today. Full text of the article can be found at: http://apps.americanbar.org/buslaw/blt/content/2012/11/article-02-voss.pdf

Statement from PEDS Co-Chairs

The PEDS Committee is focused on assisting in the education of international law practitioners on the evolving international laws and practices relating to privacy and data protection, and their application to global e-business. We also contribute to the development of policy and the promotion of the rule of law in this area. We are proud of the contributions our committee members have made to the international dialogue this year, and are planning additional programs and publications for 2013 on conducting business globally while navigating the often conflicting data protection regulatory landscape. We have bi-weekly committee meetings by conference call and would greatly welcome interest from any members of the Section who would like to participate on PEDS Committee activities. Special thanks to Katherine Woodcock and to our other contributors for putting together our Newsletter.