On September 23, 2013, California Senate Bill 568 (the “Bill”) was approved by the California Governor and filed with the Secretary of State of California (Chapter 336, Statutes of 2013), adding Chapter 22.1 on Privacy Rights for California Minors in the Digital World to Division 8 of California’s Business and Professions Code, relating to the Internet. The Bill was passed in the California Assembly on August 26, 2013, and passed with the Assembly's amendments in the California Senate on August 30th. It was presented to the Governor on September 5, 2013.

The Bill is aimed at protecting minors, who are defined as natural persons under 18 years of age who reside in California (Section 22580 (d)). Its operative provisions will come into force on January 1, 2015.

The Bill is divided into two major parts: the first prohibits certain advertising and marketing of designated products and services to minors (Section 22580 – which also contains definitions), and the second provides a digital “eraser” right or “right to be forgotten” for minors – which may be a “first” in the United States.

Prohibitions of Certain Advertising and Marketing of Designated Products and Services to Minors

Breaking down the first major part, the Bill prohibits an operator (“Operator”) of an Internet Web site, service or application or a mobile app (“Media”) directed to minors from marketing or advertising certain products or services on such Media; however, if the marketing or advertising is carried out by an advertising service and the Operator informs it of the Media being directed to minors, the operator will be deemed in compliance with the law and the advertising service will be prohibited from advertising or marketing such products or services on the Media. The Bill also prohibits such an Operator from directly marketing or advertising such products or services to a minor who he has actual knowledge is using such Media, based upon information specific to the minor, such as the minor’s profile, activity, address, or location which enables him to contact the minor (but excluding the IP address or product ID numbers for the operation of the service); however, the Operator will be deemed to comply with this prohibition if he takes reasonable good faith actions to avoid marketing or advertising in these prohibited circumstances. Next, such an Operator, if his Media is directed to minors or who has actual knowledge that they are being used by minors shall not knowingly use, disclose, compile a minor’s personal information or allow a third party to do the same, with actual knowledge that such use, disclosure or compilation is for the
Ireland and US Sign MOU on Data Protection Cooperation

By Rob Corbet, Partner at Arthur Cox

Amid all the noise around the Prism controversy, there was relatively little coverage of the news that the Irish Data Protection Commissioner (“DPC”) has entered into a Memorandum of Understanding (“MoU”) with the US Federal Trade Commission. The MoU is an interesting expression of the DPC’s intention to pro-actively work to overcome perceived EU-US privacy impediments while working within the confines of the EU Data Protection regime.

The MoU

The MoU is entitled “Memorandum of Understanding between the United States Federal Trade Commission and the Office of the Data Protection Commissioner of Ireland on Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector”. It was signed in Washington DC by the DPC, Mr. Billy Hawkes, and by the Chairwoman of the FTC, Ms. Edith Ramirez, on 26 June 2013.

The idea of a bilateral MoU between Ireland and the US is an innovative one and is to be welcomed. For those of us who believe that the EU’s restrictive approach to data transfers is unduly bureaucratic, it was heartening to see that even within the confines of the existing Data Protection regime, explicit cross-border cooperation is possible.

Legislative Basis

The MoU shows that the absence of any global data protection legislative standards does not mean that states cannot get on with the business of regulating business realities. The MoU expressly recognizes that the nature of the modern global economy requires the increase in the flow of personal information across borders, as well as the increasing complexity and pervasiveness of information technologies and the resulting need for increased cross-border enforcement cooperation. However, rather than continuing the EU-US Mexican stand-off on data protection, the two States have identified areas where cross-border cooperation was possible and in the public interest. In particular, the U.S. Federal Trade Commission Act, as amended by the U.S. SAFE WEB Act enables the sharing of data with overseas regulators, while Section 15 of the Irish Data Protection Acts 1988 and 2003 enables the DPC to do the same (indeed this mutual co-operation principle goes back to the 1981 Strasbourg Convention, which is appended to the DPAs). Given both the US and Ireland have a shared interest in protecting the privacy of their citizens and given that huge amounts of data that are transferred between Ireland and the US, it makes sense that the two states would adopt a public position on how they intend to cooperate in areas of shared interest.

Scope

The MoU is modest enough in its scope in that it is not legally binding and applies only to practices that would violate privacy laws that are the same or substantially similar in both countries. However, both sides do commit to using their "best efforts" to share information and provide investigative assistance where priority privacy violations are identified. Efforts will focus on violations which are most serious in nature. Interestingly the MoU refers not to violations involving potential financial loss, but rather to violations that cause or are likely to cause “injury to a significant number of persons, and those otherwise causing substantial injury”. A procedure is documented for effecting this cooperation.

The approach of the DPC and the FTC to try to address a genuine issue of enforcement stands in stark contrast to the broader EU-US arguments on data protection.

Prism/Safe Harbor

Much of the debate on EU/US data transfers tends to get wrongly presented in absolute terms. This has become all the clearer in the context of the Prism controversy which EU Commissioner Reding has
marketing or advertising certain products or services to such minor. The certain products or services referred to above are the following:

- Alcoholic beverages
- Firearms or handguns
- Ammunition or reload ammunition
- Handgun safety certificates
- Aerosol containers of paint capable of defacing property
- Etching cream capable of defacing property
- Various forms of tobacco and smoking products, preparations, and paraphernalia including cigarette papers
- BB devices
- Dangerous fireworks
- Tanning in an UV tanning device
- Dietary supplements containing ephedrine group alkaloids
- Tickets or shares in a lottery game
- Salvia divinorum or Salvinorin A, or substances or materials containing them
- Body branding
- Permanent tattoos
- Drug paraphernalia
- Electronic cigarettes
- Obscene matter; and
- Less lethal weapons

The actual text of the Bill should be consulted for more details regarding the advertising or marketing subject to these prohibitions.

A Digital “Eraser” Right or “Right to Be Forgotten” for Minors

The second major part of the Bill provides that an Operator of a Media directed to minors or one who has actual knowledge that a minor is using its Media, shall do all of the following:

1. Allow a minor who is a registered user of the Media to remove or, if preferred by the Operator, request and obtain removal of, content or information posted on the Media by the user.
2. Provide notice to such minor of such right to remove or to request removal.
3. Provide clear instructions to such minor on how to exercise such right to remove or to request removal.
4. Provide notice to such minor that the removal described in point 1 above does not ensure complete or comprehensive removal of the content or information posted on the Media by the user.

Under the Bill, an Operator or third party is not required to erase or eliminate content or information, or to enable the erasure or elimination of the same, in certain circumstances:

- Where federal or state law requires it to maintain the content or information.
- When the content or information was stored on or posted to the Operator’s Media by a third party other than the minor, who is a registered user, including content or information posted by the registered user that was stored, republished or reposted by the third party.
- If the Operator anonymizes the content or information posted by the minor who is a registered user, so that the minor cannot be individually identified.
- When the minor does not follow the instructions mentioned in point 3 above on how to exercise the right to remove or to request removal.
- Where the minor received compensation or consideration for furnishing the content.

Law enforcement officers may still be able to obtain content or information from an Operator under law or by court order. An Operator is deemed in compliance with the second major part of the Bill: (i) if the content or information is made invisible to other users and the public, even though it may still be on the Operator’s servers; or, (ii) if in spite of (i) above, the content or information remains visible because a third party copied it or reposted it.

Finally, despite the crucial age-based definition of
MOU on Data Protection Cooperation

Continued from page 2

recently referred to as a “wake-up call" to increase the pace for European data protection reform. It has led to strong statements from Commissioner Reding that the Safe Harbor regime “may not be so safe after all" having become a “loophole for data transfers because it allows data transfers from EU to US companies – although US data protection standards are lower than our European ones”. The Commissioner’s response is to advocate a “solid assessment of the Safe Harbour Agreement" that she intends to present before the end of the year.

For US companies trying to operate in Europe this must come as a depressing development. Previous initiatives from the Commission relating to data transfers, such as Model Clauses and Binding Corporate Rules, represented little more than a victory of bureaucracy over substance. For many US companies, who aspired to comply with EU data protection standards, the Safe Harbor at least offered a more realistic and systematic means of enabling the free flow of information to US servers. That route is now under attack with some EU Member States, reported to be considering removing it as a means of legitimizing the transfer of data to the US.

The underlying premise that the US spying laws are radically different to those that exist in Europe is also one that should be tested. In an excellent white paper on the topic in May 2013 (before the controversy broke) entitled “A Sober Look at National Security Access to Data in the Cloud" Winston Maxwell and Christopher Wolf of Hogan Lovells debunked the theory that EU States are a bastion of privacy over law enforcement. They point out, for example, that a 1991 law in France allows for no court involvement in data interceptions which are kept secret while, in Germany, the Federal Office of Criminal Investigation, the Bundeskriminalamt, has authority in investigations that concern national security or terrorism to use a computer virus to search IT systems, monitor ongoing communications and collect communication traffic data without the knowledge of data subjects or service providers. Similarly in the UK, the Tempora scheme has recently been revealed to involve the secret monitoring of large volumes of Internet data.

This being the case, how can Prism be a “wake up call" for the EU Commission and, if we take away the Safe Harbor, does the EU really believe that data transferred to the US under “Model Clauses" or BCRs is really any better protected?

The Irish Data Protection Commissioner is to be congratulated in trying to cooperate with the FTC to improve data governance in the interests of citizens despite the backdrop of EU-US political intransigence and moral posturing.

French Procedure against Google for Data Privacy Violations

By W. Gregory Voss, Toulouse University, Toulouse Business School (TBS)

The French data protection agency – the CNIL (Commission Nationale de l'Informatique et des Libertés) – announced on September 27, 2013, after Google Inc. contested an order to comply with French law on the last day of the three-month period for such compliance, that it is initiating a formal procedure, which may lead to sanctions against Google Inc. for breaches of paragraph II of Article 32 (Obligations Incumbent upon Data Controllers and Rights of Individuals – Rights of Individuals) of France’s data protection legislation (“the French DP Law”).

The French order and the other enforcement action relate to Google’s global privacy policy which was introduced in March 1, 2012 (and last modified on June 24, 2013). From February through October 2012, Google’s Privacy Policy, which replaced individual privacy policies for the various Google services, was the subject of correspondence between the Article 29 Working Party, of which the CNIL is a
French Procedure against Google

member, and Google. In these Google’s then-new Privacy Policy was said not to comply with EU data protection law, especially in connection with information requirements regarding the purpose of data collection and the use of such data, which were then bundled together in one privacy policy although the purpose and use of data collection might differ from service to service. The CNIL was given the lead role to discuss with Google the privacy issues that arose under the Google Privacy Policy.

On October 16, 2012, the Article 29 Working Party set out recommendations for Google to take to upgrade its privacy policy practices, contained in an Annex to a letter to Google, with which Google was asked to comply within four months. After the expiration of the four-month period, without implementation by Google of “any significant compliance measures”, six European data protection authorities announced on April 2, 2013 that they had launched enforcement actions against Google.

The CNIL stated that the six data protection authorities base their enforcement actions on similar breaches: “insufficient information”, “undefined or insufficiently defined data retention periods” and “unlimited combination of data”. It highlighted that, although in each case the actions are based on a European directive, European “national data protection laws are slightly different”.

The procedure initiated on September 27, 2013 under Article 46 of the French DP Law involves the appointing of a rapporteur to prepare a report, which should then be notified to Google Inc. who may then submit its remarks before the report goes to the Select Committee of the CNIL for a decision on the sanctions to be assessed. The Select Committee’s decision must include the reasoning on which it is based and be notified to the data controller (Google Inc.). Following this, an appeal is possible to France’s highest administrative court – the Conseil d’Etat (Council of State).

Possible sanctions under Article 45 of the French DP Law, after hearing the parties, exceed the period necessary for the purposes for which they are collected;
• Not proceed, without legal basis, with the potentially unlimited combination of users’ data;
• Fairly collect and process passive users’ data, in particular with regard to data collected using the “Doubleclick” and “Analytics” cookies, “+1” buttons or any other Google service available on the visited page;
• Inform users and then obtain their consent in particular before storing cookies in their terminal."

“The CNIL’s June 20, 2013 order to comply with French law was part of this larger set of enforcement actions taken simultaneously in six EU countries: France, Spain, UK, Germany, the Netherlands and Italy.”
French Procedure against Google

include the following:

- A financial penalty under the Article 47 of the French DP Law (€150,000 maximum in case of a first breach and up to €300,000 “where similar previous offences have been committed”)
- An injunction to cease the processing

The CNIL’s Select Committee may make the sanctions public and order their publication in the journals, newspapers or “other media” it designates at the sanctioned party’s expense.

It remains to be seen the sanction that the CNIL will impose upon Google. It should be noted that the CNIL imposed a €100,000 fine on Google in 2011 for violation of the French DP Law.

Endnotes:

9 CNIL orders Google to Comply, op cit. In 2.
11 French DP Law, op. cit. fn. 3, art. 46, at 34. 12 Id., art. 47, at 34.
14 French DP Law, op. cit. fn. 3, art. 45, at 34.
15 Id., art. 46, at 34.

Privacy, E-Commerce & Data Security Committee - Quarterly Newsletter

Continued from page 5
Right to Be Forgotten

Continued from page 3

of “minor” mentioned above, nothing in the second major part of the Bill requires an Operator to collect user age information.\textsuperscript{12}

Time will tell if other States will follow California’s lead in allowing minors a right to be forgotten, or whether this right will eventually be extended to adults, as well.

Endnotes:

\textsuperscript{1} CA Sen. Bill 568, Privacy: Internet: minors

Update to the OECD Guidelines

On July 11, 2013, the OECD issued its revised Privacy Guidelines – the first update to the original 1980 Guidelines. The revised Guidelines include 1) Recommendation of the OECD Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data and 2) explanatory memorandum on the revisions.

Echoing concerns involved in the revision to the EU’s data protection and privacy framework, the focus of the revision is on the practical and risk-based approach to the implementation of privacy as well as the need for better interoperability. The revised Guidelines and memorandum can be accessed at\textsuperscript{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12} www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.


Results from International Conference of Data Protection and Privacy Commissioners

The 35th annual International Conference of Data Protection and Privacy Commissioners took place September 23-26 in Warsaw, Poland. One focus of this year’s conference was on the coordination of cross-border investigation and privacy enforcement in certain situations.

The resolution on enforcement coordination is available at\textsuperscript{20} https://privacyconference2013.org/web/pageFiles/kcfinder/files/4.%20Enforcement%20coordination%20resolution%20EN%20.pdf, with the anticipation of a multilateral framework document to be adopted at next year’s conference.

Additionally, a declaration was passed regarding apps, “Warsaw Declaration on the “Applification of Society” see https://privacyconference2013.org/web/pageFiles/kcfinder/files/ATT29312.pdf.

All of the conference’s resolutions and declarations can be found at https://privacyconference2013.org/Resolutions_and_Declarations.
Committee News & Events

(Co-)Sponsored Programs in London

- “Where In The World Is Your Evidence? The Challenges of Gathering Electronic Information Worldwide For Litigation, Arbitration and Investigations”, Thursday, October 17, 2:30 pm – 4:00 pm
- “Social Media: A Web of Challenges”, Thursday, October 17, 9:00 am – 10:30 am

Attending the SIL 2013 Fall Meeting in London?

Meet and discuss with the Committee in person!

We are having a Committee Meeting in London (Spectra Suite) on Friday October 18 from 8:15 AM to 9:15 AM. Please do drop by if you are attending the London Meeting.

Call for Authors for the PEDS YIR 2013

The time has come to participate in drafting The Year-in-Review (“YIR”) edition for 2013. The YIR is prepared in cooperation with the SMU Dedman School of Law. Late each spring the Section of International Law publishes the YIR based on submissions from all the Section's committees. This is a great way to get some exposure for you and your organization. We are therefore requesting you to consider submitting a short update of the most significant legal developments in your specialized area of privacy, e-commerce and data protection law for the year 2013.

Written submissions should be no more than 500 words, including footnotes, and each should have one author, although credit for research may be given in a footnote. The submission must be drafted in a law review format. Submissions may have to be edited in order to comply with the YIR's strict word limits.

If you are interested in submitting something, please respond to Committee Editor Gregory Voss (g.voss@tbs-education.fr) in order to express your interest no later than Friday, October 18, 2013. If you are in London for the Fall Meeting you may tell Greg there!

As part of your response, please provide a brief description of the topic you intend to cover (including geographic area), your name, e-mail address and telephone number.

Contributions from last year are available at http://www.americanbar.org/content/dam/aba/publications/international_lawyer/ti_l_47_1/privacyscommerceanddatasecurity.authcheckdam.pdf (sign-in required), in order to see form, citation style, etc.