NEW FRENCH COOKIE GUIDANCE SET REALISTIC RULES: FOR USER’S PRIOR INFORMATION AND CONSENT

By: Christophe Héry, Avocat au Barreau de Paris, Associé/Partner

The French Data Protection Agency, the CNIL (Commission Nationale Informatique et Libertés), issued in December 2013 a new set of guidelines relating to the use of cookies.

The legal framework

Pursuant to the EU “e-privacy” Directive no. 2002/58/EC of 12 July 2002, supplemented by EU Directive no. 2009/136/EC, internet operators must give internet users clear and exhaustive information on the use of cookies and get their prior consent before implementing them. The EU Directive was transposed into French law by article 32-II of the Act of 06 January 1978 (the French Data Protection Act). The goal of the CNIL’s resolution (no. 2013-378) of 05 December 2013, completed by a FAQ and informations leaflets, is to clarify the terms of application of article 32-II. It aims at finding a just balance between user protection and website or application operation.

A wide scope as regards the types of cookies, the data and the operators

The resolution indicates that article 32-II of the French Data Protection Act covers all cookies and any other tracking technology enabling operators to directly or indirectly identify users, their needs, their surfing habits, etc. Therefore, are covered, for instance, in addition to HTTP cookies, all flash cookies, advertising cookies, tracking cookies used or installed when visiting a social network or a website or when downloading an application. There are three exceptions: those whose sole purpose is to enable or facilitate communication by electronic means, those that are strictly necessary in order to provide an online communication service expressly requested by a user (e.g., authentication cookies and cart cookies) and those used for audience analytics.

Article 32-II covers cookies giving access either to personal or non-personal data.

The rules also apply to all internet professionals: website or mobile application publishers and all their partners such as advertisers, social network managers,

See, “New French Cookie”, page 3
Google Assessed Highest French Fine in Privacy Policy Case

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

In the Summer 2013 quarterly issue of the Privacy, E-Commerce & Data Security Committee Newsletter, we reported on the “French Procedure against Google for Data Privacy Violations” (pages 4-6). On January 3, 2014 the Sanctions Committee of the French Data Protection Authority (CNIL) handed down its decision in the case of Google’s new privacy policy, ordered the latter to pay the highest fine available for a first offense -- €150,000 (Deliberation No. 2013-420 (Deliberation) of the Sanctions Committee of CNIL imposing a financial penalty against Google Inc., available translated into English on the website of the CNIL – www.cnil.fr). The Deliberation was rendered under Article 45(I) of France’s Data Protection Act (Loi 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers, et aux libertés [Law 78-17 of Jan. 6, 1978 on Information Technology Data Files and Civil Liberties], available in translation on the CNIL’s website.

The CNIL cited many ways in which Google failed to comply with the French law: insufficient information to users regarding the processing of their personal data, not obtaining user consent prior to placing cookies on their terminals (e.g., computers or mobile device such as tablets or smart phones), combining data from its different services without a legal basis for doing so, etc.

The Deliberation included an order that Google publish the decision for a period of forty-eight (48) consecutive hours on its French home page (www.google.fr), under the “Google search” and “I’m feeling lucky” buttons, and above the cookie information banner, together with a link to a page on the CNIL’s website (http://www.cnil.fr.institution/missions/sanctionner/Google/).

See, “Google”, Page 3

“2014 PEDS Survey”

2013 was a significant year in global data protection with the emergence of the Snowden revelations and wide media attention on the ramifications for data privacy laws in the US, Europe and beyond. In light of this, we asked some PEDS Committee members to participate in a survey to predict how they see 2014 playing out. Here is what they said:

What do you think are the main implications of the PRISM Controversy on the regulation of personal data in the United States and abroad?

Answer 1: “The controversy has highlighted privacy concerns associated with US tech businesses and storing information in the U.S. – also for U.S. businesses and citizens. It has shined light on data privacy, confidentiality and security issues that were previously touted by only marginal groups. Ordinary citizens both in the US and abroad now have a heightened awareness about government surveillance. Moreover, they can concretely see how government surveillance affects them – it is no longer a distant theoretical possibility.”

“In Europe, one can already see that the political controversy has further entrenched EU positions on data protection. It has also strengthened the arguments of those who want to push through the General Data Protection Regulation as soon as possible. Furthermore, the controversy has solidified the stance of many within the EU that it should be developing its own data centers and technology base to rival that of the U.S. and Asia. The objective would be twofold: 1) protecting Europeans’ personal data and 2) economic growth and development in the technology sector (supporting the EU’s “Digital Agenda”)”
“NEW FRENCH COOKIE”

A pragmatic approach to the user’s prior information and consent

**In principle:** The prior information must be comprehensive, clearly visible and be expressed in simple terms that the average user can understand. As a consequence, legal or complex technical terminology are ruled out. For their part, users are deemed to have consented to the cookies if they carry on surfing on the website concerned.

**In practice:** Most of the time, the information takes the form of a banner displayed on the screen that states (i) what the specific purpose of each cookie used is, (ii) how users can oppose the use of cookies and change the cookie settings by clicking on a link displayed on the banner, and (iii) how they can give their consent. CNIL reserves the right to monitor how really the information is given and consent secured (in a user-friendly way).

After being given the information, users have three options:

- **quitting the website** they are viewing, in which case they may not in any case have given their consent to the use of cookies, or
- **carrying on surfing,** which equates with clearly and unambiguously consenting to the installation and use of cookies, or
- **refusing the installation of** cookies and clicking on a link (eg “For more information”) to open the cookie settings in order to reject them or change their settings after being advised in simple and intelligible terms.

CNIL suggests **thirteen months** as the maximum lifespan for the consent given by each user (instead of six months under the former guidelines) at the expiration of which, users must again be asked to give their consent.

**Compliance v. sanctions**

It is in the interest of all internet professionals using or operating cookies to comply spontaneously with these rules since users are clearly informed by CNIL of their rights and help them identify internet marketing professionals in breach of these rules. Then, besides the sanctions (especially in the form of fines) that CNIL has authority to hand down, judgment of internet users with regard to how internet operators treat their privacy should push the latter to quickly implement the practical solutions set out in the French DPA Act and recommended by CNIL.

---

**2013 Survey Results**

Answer 2…

“The immediate focus is on the integrity of the Safe Harbor regime. It seems likely that the self-certification element of safe harbor will continue to come under further scrutiny as more examples emerge of companies not properly adhering to the regime (e.g. the recent FTC charges against Bittorrent and other companies). More broadly however, it will be interesting to see how EU Member States and the US itself address the key issue of communications surveillance. What has been largely lost in the debate so far is the fact that most EU member states have national surveillance laws of their own and the extent to which they are used is not as transparent as the EU Commission might seem to imply.”
“Although the financial penalty handed down by the CNIL is France’s largest to date, it is nothing compared to Google’s worldwide annual turnover.”

Google…

On January 13, 2014, Google appealed the publication aspect of the Deliberation in summary proceedings (en référé) to France’s highest administrative court – the Council of State (Conseil d’État), which rejected the summary proceedings motion in an order on February 7, 2014 (Ordonnance du 7 février 2014, Société Google Inc., N° 374595), thereby requiring Google to comply with the publication order. Google has also filed an appeal in parallel in full trial proceedings (sur le fond), although this did not stop the execution of the publication order (see the website of the Council of State: www.conseil-etat.fr).

Although the financial penalty handed down by the CNIL is France’s largest to date, it is nothing compared to Google’s worldwide annual turnover, or the maximum 2% of such figure that could be assessed under the European Commission’s Proposed General Data Protection Regulation (GDPR) or the even greater 5% of turnover figure of the current EU Parliament LIBE Committee draft of the GDPR.

Answer 1: “There will be a new law within the EU on Data Protection. Most companies would like to see it in the form of a Regulation as this would promote uniformity throughout the EU member states. There are however certain aspects of the law - particularly about cooperation between member states - that support keeping the law as a Directive. It is very difficult to predict and thus derive legal certainty about what the data protection regime will look like under a Regulation.”

Answer 2: “Under the Irish Presidency of the EU in 2013 there was a huge push to progress the draft Regulation. However, the momentum was lost when the LIBE Committee re-opened a number of issues so Commissioner Reding’s goal of having the Regulation enacted prior to the European elections in May 2014 has been lost. Some member states such as the UK continue to favour a Directive over a Regulation. The distinction is important as one of the main advantages being sold by the EU was that a Regulation (i.e. a single law with direct effect across the EU) would overcome the complexities that currently arise under the 1995 Data Protection Directive (which has been transposed in significantly different ways across the EU member states). It will be fascinating to see how the new Commission and Parliament confront the issue. So much preparatory work has been done, it seems unlikely that some form of significant updating of EU data protection laws will not be in place within the next 1 – 3 years.”
2013 Survey

Answer 2: “Safe Harbor will survive. Will it be the same regime as it was in historically? No. Since the EC has called on the U.S. to “restore trust”, we have already seen the FTC stepping up enforcement actions against companies falsely claiming to comply with Safe Harbor. This pattern of enforcement will continue and create greater consciousness within Safe Harbor certified companies. The U.S. will not meet all the demands laid out in the Report, such as the call to accede to the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (so-called “Convention 108”). The reaction in the U.S. should be a clear one: it should actually do what it signed on for and ensure that Safe Harbor certified companies’ policies and practices reflect the same. “

Answer 1: “Aside from the EU legislative developments, there will be an proliferation of information security standards globally. These security standards will continue to develop and one will see an increase in uniformity and global focus on them. Given the recent data breaches and focus on cybersecurity, data protection will clearly benefit from this development.”

Answer 2: “For Ireland, our Data Protection Commissioner, Billy Hawkes is due to retire from the office in 2014. He has been a hugely influential figure internationally given Ireland’s position as European hub for so many of the world’s most significant data controllers. His successor will face the delicate challenge of continuing to offer a pragmatic data protection compliance environment within a new regulatory regime and under the glare of privacy groups and the world’s media.”

Litigation Committee Joint Project

The Intl Litigation Committee’s Data Privacy Working Group is undertaking a project which consists of a jurisdiction by jurisdiction survey of the rules governing the access, use and transfer of personally identifiable information (PII) for the purposes of cross-border litigation.

The goal is to produce a comprehensive and practical data protection guide for litigators for use around the world. This survey addresses all relevant issues which a litigator might face when attempting to gather evidence which would fall under the data privacy protection rules in a given jurisdiction.

The preliminary framework of this project has already been put in place by the members of the International Litigation committee but the input and contributions of PEDS committee members would be greatly appreciated. This joint project offers the PEDS committee members who participate the opportunity to showcase their expertise to a larger community of lawyers and legal counsel.

Please direct all inquiries to Brendan Berne, vice-chair of the PEDS and International Litigation committees, at bberne@piton-gillespie.com.
The PEDS committee would like to take this opportunity to thank the volunteers who agreed to assist in the adjudication of the Rona Mears writing competition to encourage law student interest and participation in the practice of International Law and the Section. This year, the topic is Edward Snowden and students were asked to address either (1) why Mr. Snowden is, or is not, guilty of violating U.S., foreign or international laws or (2) why the U.S. Government has, or has not, violated U.S., foreign or international law through its actions disclosed by Mr. Snowden. Our thanks go to Gregory Voss, Sunita D. Doobay, Cecil Saehoon Chung, Julian Shepard and Karen Woo for offering to assist as adjudicators.

PEDS Mission Statement

The Privacy, E-Commerce and Data Security Committee has been established as a resource to assist in the education of international law practitioners on the evolving international laws and practices relating to privacy and data protection, in particular as they relate to global e-business, and to contribute to the development of policy and the promotion of the rule of law in those areas.

Committee News

* Gregory Voss, Professor at Toulouse Business School and Vice-Chair of the PEDS Committee co-authored “Céline Castets-Renard and Gregory Voss, “Le ‘droit à l’oubli numérique’ en Europe et en Californie”, Revue Lamy Droit de l’Immatériel No. 100, pp. 51-55 (January 2014). (This is a Wolters Kluwer France publication.)

From April 1-5, 2014, Privacy, E-Commerce and Data Security (PEDS) Committee members will be attending the ABA Section of International Law’s Spring Meeting 2014, based at the Waldorf-Astoria Hotel. The PEDS Committee has co-sponsored several panels at the Spring Meeting, as indicated below:

**Wednesday, April 2, 10:45am – 12pm** “Employees In the Digital World: The Employer’s Best Line of Defense and Greatest Threat to Data Security”

**Wednesday, April 2, 3:45pm – 5pm** “The New Frontline is Online: Are Your Defenses Ready?”

**Thursday, April 3, 10:45am – 12pm** “Balancing Global Trends in Privacy and Data Protection: Keeping Up with Developments in U.S., Europe and Asia” - The PEDS Committee is the primary sponsor of this panel and it will be represented on the panel by PEDS Co-Chair Katherine Woodcock as Moderator and PEDS Vice-Chairs Cecil Saehoon Chung and Gregory Voss as Speakers.

Please put these panels on your meeting calendar!

In addition, the PEDS Committee will be holding a Committee Dinner at a location to be determined on Thursday evening, April 4. All interested in attending the PEDS Committee dinner should contact Katherine Woodcock by e-mail (katherinewoodcock@hotmail.com).

A Big “Thank you”…

The PEDS committee would like to take this opportunity to thank the volunteers who agreed to assist in the adjudication of the Rona Mears writing competition to encourage law student interest and participation in the practice of International Law and the Section. This year, the topic is Edward Snowden and students were asked to address either (1) why Mr. Snowden is, or is not, guilty of violating U.S., foreign or international laws or (2) why the U.S. Government has, or has not, violated U.S., foreign or international law through its actions disclosed by Mr. Snowden. Our thanks go to Gregory Voss, Sunita D. Doobay, Cecil Saehoon Chung, Julian Shepard and Karen Woo for offering to assist as adjudicators.