ALSTON & BIRD LLP

WWW.ALSTON.COM

Privacy & Security ADVISORY ■

OCTOBER 2, 2014

European Data Protection Authorities to Ramp up Enforcement of Cookie Rules

By Dominique R. Shelton and David Caplan

In her speech addressing the Lex Mundi Intellectual Property Section (at the invitation of member Alston & Bird) on Friday, September 26, 2014, Florence Raynal, head of France's data protection authority, Commission Nationale de L'informatique et des Libertés (CNIL), made it clear that France and other European countries would be focused on coordinated efforts to enforce privacy rights for individuals, including between the European Union (EU) and the United States, France and the Asia-Pacific Economic Cooperation (APEC), and France and Francophone countries. The focus will be on issues surrounding notice to consumers regarding the data collected about them, enforcement in the areas of cookies, and cybersecurity/data breach more broadly.

In hearing Ms. Raynal's remarks, Alston & Bird gleaned the following takeaways:

- European regulators will focus on heightened "transparency" to consumers
- The new proposed amendments to the EU privacy directive will focus more on the right of portability of personal information by consumers
- The so-called "right to be forgotten" that was the focus of the recent case decision against Google in Spain/EU will continue to be a focus.

If these remarks are any guide, new obligations for data controllers should be anticipated.

On the positive side, there should be fewer administrative filings necessary if the new amendments to the EU privacy directive are ultimately adopted. On the other hand, the following more onerous obligations on business should be expected: (1) more obligations for data controllers/processors; (2) companies will need to put mechanisms in place to "demonstrate compliance"; (3) there will be a renewed focus on accountability through accreditation and proof that internal best practices are in place; (4) before taking on new projects that implicate privacy, companies will need to develop a Privacy Impact Assessment; (5) companies should expect Europe-wide security breach obligations—above and beyond the telecom sector that already exists in France; (6) companies will soon be obligated to appoint a company data protection officer; (7) training will become a must; (8) with the new EU privacy directives, while currently CNIL cannot sanction more than €100,000 ($127,000), the new proposed amendments would permit fines from anywhere between 2 and 5 percent of a company's revenues; and last, but not least, (9) tracking technologies like cookies will continue to be a focus of regulatory enforcement across Europe *working in conjunction with* U.S. enforcers such as the Federal Trade Commission (FTC).

From September 15-19, 2014, European data protection authorities conducted "Cookies Sweep Day" audits to compare and verify the implementation of cookie notice and consent rules for websites that target users in the European Union. The purpose of the audit is primarily to gather information for the Article 29 Data Protection Working Party (also called G29), an advisory group for the European Commission. However, Cookies Sweep Day reflects a trend toward greater enforcement by European data protection authorities, including France's CNIL, which announced on July 11, 2014, both its participation in the Cookies Sweep Day and its own October audit that may result in notices and sanctions against organizations that fail to comply with cookie notice and consent rules.

Cookie Notice and Consent Rules

Broad principles relating to storing information on users' computers are outlined in Article 5(3) of Directive 2009/136/EC of the European Parliament (amending Directive 2002/58/EC). Article 5(3) requires publishers to get a user's consent before it stores or accesses information, like a cookie, on a user's computer. Moreover, publishers must provide a clear notice of the cookie's intended purpose. Article 5(3) makes an exception to the notice and consent requirements for cookies that are necessary to provide a service explicitly requested by the user or whose sole purpose is to enable electronic communications.

Data protection authorities of EU countries have issued formal guidance for complying with Article 5(3), including the CNIL's recommendations on December 16, 2013, which state that a user must be informed and give consent prior to the installation of some cookies. The guidance calls for getting user consent in a two-step process:

- Provide a banner on the site informing users that further navigation on the site constitutes an agreement to accept the site's cookies. The banner, placed on the homepage or secondary pages, must specify the purpose of the cookies used on the site and provide a means for rejecting the cookies. The banner should not disappear until the user navigates off the page (e.g., from the homepage to a subpage).
- The user must be given clear instructions regarding how to accept or reject all or some cookies.

The recommendations state that the publisher's website cannot install the cookies until the user continues navigating the site or accepts the cookies. The CNIL guidance specifies certain kinds of cookies for notice and consent requirements, including cookies related to transactions for targeted advertising, cookies generated by social network "share" buttons that collect personal data, and analytics cookies. However, the guidance also lists examples of cookies that meet the requirements for exemption under Article 5(3), including certain session, authentication and shopping cart cookies.

CNIL Cookies Audit

In addition to the September Cookies Sweep Day audits, the CNIL announced on July 11, 2014, that it will also conduct audits in October 2014.

The CNIL audit will analyze:

- The type of tracking used by websites (e.g., HTTP cookies, local shared objects or fingerprinting).
- The purposes of the cookies on a website: whether the publisher knows the purpose of all the cookies installed by or read from its site, internal or "third party," and whether there are cookies without a purpose (e.g., obsolete cookies).
- If the purpose of certain cookies requires a user's consent, the CNIL will also examine:
  - How the site obtains the user's consent: whether the cookies requiring consent are installed or read prior to the user giving consent (e.g., when the user first arrived at the homepage); how the user expresses consent (e.g., clicking a button, continuing navigation through the website after reading the notice banner, etc.); or whether the consent mechanism is user friendly.
  - The visibility, quality and simplicity of information concerning the cookies.

- The consequences of a user refusing to accept cookies that require consent, for example on an e-commerce website, whether the site offers options for refusing cookies or forces the user to block all cookies, thus preventing the user from making purchases from the site.
- The possibility of withdrawing consent at any time.
- The expiration of the accepted cookies (the CNIL's recommendation is a maximum lifespan of 13 months).
- Issues related to cookies will also be reviewed, such as data security and the presence of sensitive data.

Will the Audit Lead to Sanctions?

According to the CNIL July 11 announcement, the CNIL may issue formal notices or sanctions against publishers that have not complied with the CNIL's recommendations. Enforcement by the CNIL reflects the recent stepped up enforcement activity by other European data protection authorities.

The CNIL's sanctions committee issued a €150,000 ($190,500) penalty against Google in January 2014 for failing to comply with the EU legal framework and the French Data Protection Act. This enforcement focused on Google's privacy policy, but also related to Google's implementation of cookies–its failure to obtain user consent prior to dropping cookies on users' devices. The CNIL's action followed similar actions against Google in late 2013 by the Dutch and Spanish data protection authorities. Both of those authorities were also involved in recent enforcement actions against publishers that failed to comply with cookies rules.

On January 14, 2014, the Spanish Data Protection Authority (AEPD) fined two companies that violated the Spanish data protection laws concerning cookies. The AEPD fined jewelry companies Navas Joyeros Importadores, S.L., and Privilegia Luxury Experience, S.L., because the cookie information on each company's website was incomplete and unclear, thus invalidating any consent provided by users in accepting the "Cookies Policy" or by continuing to browse the websites.

On May 13, 2014, the Dutch Data Protection Authority (CBP) published a report on its investigation into YD Display Advertising Benelux. The report concluded that YD violated cookie rules by dropping and reading cookies without adequate information and prior consent from users. YD did not ask permission to install cookies–it only provided users a means for opting-out of receiving personalized ads. The DPA determined that YD's cookies tracked personal data, and under Dutch telecommunications and data protection laws, the processing of personal data requires prior unambiguous consent. Dutch laws also have the presumption that using tracking cookies constitutes the processing of personal data.

On July 31, 2014, another Dutch authority, the Netherlands Authority for Consumers and Markets (ACM) determined that Netherlands Public Broadcasting (NPO) violated cookie rules in the Dutch Telecommunication Act, subjecting NPO to periodic penalty payments if it does not address the violations. The penalties would range from €25,000 to €125,000 per week ($37,700 to $185,700). NPO had been storing cookies without the informed consent of its users. This action followed notifications sent to various government websites in 2012 concerning compliance with Dutch cookies rules.

Data protection authorities throughout the EU have been moving rapidly in the last year toward a sanctioning regime, finding that websites have had long enough to comply with the data protection acts.

Alston & Bird's Data & Privacy Group will continue to monitor developments in this area and advise as other EU data protection authorities weigh in on this issue.

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Security Group

Atlanta

Angela T. Burnette
angie.burnette@alston.com
404.881.7665

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

Lisa H. Cassilly
lisa.cassilly@alston.com
404.881.7945

Maki DePalo
maki.depalo@alston.com
404.881.4280

Clare H. Draper, IV
clare.draper@alston.com
404.881.7191

Peter K. Floyd
peter.floyd@alston.com
404.881.4510

James A. Harvey
jim.harvey@alston.com
404.881.7328

John R. Hickman
john.hickman@alston.com
404.881.7885

William H. Jordan
bill.jordan@alston.com
404.881.7850
202.239.3494

David C. Keating
david.keating@alston.com
404.881.7355

W. Scott Kitchens
scott.kitchens@alston.com
404.881.4955

Dawnmarie R. Matlock
dawnmarie.matlock@alston.com
404.881.4253

Kacy McCaffrey Brake
kacy.brake@alston.com
404.881.4824

Bruce Sarkisian
bruce.sarkisian@alston.com
404.881.4935

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael R. Young
michael.young@alston.com
404.881.4288

Los Angeles

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

Katherine E. Hertel
kate.hertel@alston.com
213.576.2600

Sheila A. Shah
sheila.shah@alston.com
213.576.2510

Dominique R. Shelton
dominique.shelton@alston.com
213.576.1170

Washington, D.C.

Louis S. Dennig, IV
lou.dennig@alston.com
202.239.3215

Kimberly K. Peretti
kimberly.peretti@alston.com
202.239.3720

Eric A. Shimp
eric.shimp@alston.com
202.239.3409

Paula M. Stannard
paula.stannard@alston.com
202.239.3626

Jeffrey R. Sural
jeff.sural@alston.com
202.239.3811

ALSTON&BIRD LLP

WWW.ALSTON.COM