Skadden PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
& AFFILIATES

November 2013

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact **Stuart D. Levi** at 212.735.2750 or stuart.levi@skadden.com, or your regular Skadden contact.

* * *

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

Four Times Square
New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

New California Law Gives Minors New Privacy Rights

California continues to lead the country in enacting laws that are designed to enhance individual privacy. Pursuant to a recently enacted law (S.B. 568), starting on January 1, 2015, websites and other online or mobile services and applications (Web Properties) that are (a) directed at California residents under 18 years of age (Minors) or (b) that are operating with actual knowledge that one or more Minors are visiting or otherwise using the Web Property must provide these Minors with the following protections:

1. **Removal Right**. Minors who are registered users of Web Properties must have the ability to remove or, if the operator prefers, to request and obtain removal of, content the Minor posted on the Web Properties. These registered Minors must be provided with notice of this right along with clear instructions on how to remove or request removal of such content. The notice also must make clear that this process does not ensure complete or comprehensive removal of the content.

    a. This removal obligation does not apply if: (a) any other provision of federal or state law requires maintenance of the content, (b) the content was stored, posted, reposted or republished to the Web Property by a third party other than the Minor, (c) the content is anonymized such that the Minor cannot be individually identified or (d) the Minor receives compensation for providing the content.

    b. An operator can comply with the removal obligation if it renders the content invisible to other users but does not remove the content from its servers.

This portion of SB 568 effectively gives minors a “right to be forgotten;” a topic that is being hotly debated on a broader scale within the EU.

2. **Ban on Certain Advertising**. If the Web Property is directed at Minors, the operator may not advertise or market the following items and services: (a) alcohol, (b) firearms, ammunition, and certain other gun accessories and other weapons, (c) spray paint and etching cream, (d) tobacco or other smoking paraphernalia, (e) fireworks, (f) tanning beds, (g) tattoos, (h) lottery drawings and (i) various drug products and drug paraphernalia.

    a. If the operator simply has actual knowledge that Minors are using the Web Property, the operator must take good faith measures to ensure such products or services are not marketed specifically and directly at such Minors.

    b. The foregoing restrictions on advertising and marketing also apply to advertising services which provide services online, provided that the operator of the Web Property informs the advertising service that the Web Property is directed at Minors.

Practice Points

Although the new California law does not go into effect for more than a year, Web Properties that are geared toward Minors, or know that minors visit their sites, may need considerable time to reconfigure their Web Properties to comply with the law. This is especially true for sites that allow for contributions of user-generated content. And, while the law only applies to California residents, Web Properties may find it easier to provide a single solution rather than treating Minors differently depending on where they reside. It is important to note that S.B. 568 expressly does not require an operator of a site Web Property to collect age information about users.

Obtaining Consent to Use Cookies in the EU – New Guidance Issued

Starting in January 2013, EU member states were required to implement the EU's 2009 so-called "Cookie Directive."[1] That directive, which is an amendment to the EU ePrivacy Directive, requires end-user consent before cookies can be stored on the user's computer, smartphone or other mobile device. Such consent is only valid if the user was provided with "clear and comprehensive information" about the use of the cookie.[2] Since its effective date, however, companies have wrestled with the different compliance requirements issued by individual member states.

For example, the French data protection enforcement authority (CNIL) rejected using browser settings for consent, since those settings typically fail to draw distinctions among the various cookies served and their individual purposes. Moreover, even if a user's browser is properly configured to require consent to each cookie served, CNIL asserts that such consent may nevertheless be invalid because it is not specific and not granted based on clear and complete information provided when consent is requested.[3]

In October, an EU data protection working party sought to resolve these issues by adopting guidance to assist companies in determining how to provide sufficiently visible and appropriate consent notices.[4] Rather than design a specific mechanism, the Working Party recognized that business practices have varied widely across the EU and recommended a comprehensive approach. Specifically, the Working Party recommended that consent mechanisms adopt multiple elements of the varying practices, rather than any single practice. This might not be what companies had hoped to hear, since the guidance likely serves to raise the bar higher for obtaining valid consent.

Obtaining Valid Consent

In the guidance memorandum, the Working Party identified the following four principal elements of a valid informed consent that would satisfy applicable requirements:

- consent must be immediately visible when and at the location where consent is sought and be explicit so that when consent is obtained, it is based on the specific purpose for which such consent was required;
- consent must be obtained prior to processing;
- consent must be a clear, active affirmation of the end user's agreement and grant of consent; and
- consent must be voluntary and granted in a manner providing the end user to agree or refuse the use of cookies, free of any deception, coercion or significant adverse implications if consent is not granted.

In practical terms, this means that the notice and consent mechanism should be immediately visible as soon as a user visits the website (or enters a page from where the cookie will be placed). The notice should provide users with information specifying: (a) the type of cookie, its source and the reasons for the use of the cookie, (b) information about any data that will be collected and

[1] *See* "EU Cookie" Directive 2009/136/EC of November 25, 2009, amending Directive 2002/22/EC, Directive 2002/58/EC, and Regulation No 2006/2004, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF*and* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:241:0009:0009:EN:PDF.

[2] The Directive provides an exemption from the requirement if the cookie is necessary for the provision of a service that has been requested by the user.

[3] *See* CNIL News dated April 26, 2012, *available at* http://www.cnil.fr/english/news-and-events/news/article/what-the-telecoms-package-changes-for-cookies/.

[4] *See* Working Document 02/2013 providing guidance on obtaining consent for cookies, adopted on October 2, 2013, by the Article 29 Data Protection Working Party (the Working Party), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.

which may accessible by third parties as a result of the cookie, (c) any third-party cookies on the site, (d) the expiration date of the applicable cookies, (e) how users can denote which cookies they wish to accept or reject and (f) all other information necessary to fully educate the user in this respect. Moreover, users must receive information indicating how they can accept all or some of the cookies as well as how to opt-out of or change a prior election in the future. Until such time as consumers have had an opportunity actively and voluntarily to accept or refuse some or all of the cookies, either by checking a box indicating agreement or clicking on a "voting" button (*e.g.*, "yes/no"), no cookies should be set to users' computers or mobile devices.

Limiting Cookies in General

In addition to providing an appropriate consent mechanism, the Working Party recommends that companies take measures to limit the use of cookies and offer users the ability to refuse those cookies that track their personal data. Should users agree to tracking cookies, applicable regulations nevertheless prohibit processing personal data unless it is pertinent to the purposes for which such data was collected.[5]

Practice Point

Companies whose websites are geared toward EU residents should carefully review the notice requirements for the use of cookies and make sure that their sites are compliant.

The US-EU Safe Harbor: Not So Safe Anymore?

Companies that transfer personal information from the EU to the United States are familiar with the U.S.-EU Safe Harbor. The Safe Harbor, which went into effect in 2000, was designed to address the provision in the European Commission's Directive on Data Protection that prohibits the transfer of personal information to countries that do not meet the EU "adequacy" standard for privacy protection. Since the U.S. does not meet this standard, the U.S. Department of Commerce and the European Commission developed a "safe harbor" framework that would provide a streamlined and cost-effective means for U.S. companies to satisfy the "adequacy" requirement. Instead of entering into so-called "model contracts" that have been pre-approved by the EU or enacting corporate rules to govern data flows between the EU and the U.S., companies could self-certify to the Safe Harbor through the Department of Commerce. The Safe Harbor requires companies to certify that they adhere to a number of privacy requirements, many of which mirror the EU's own requirements, such as providing individuals with access to their data on request. Once certified, a company can receive data from the EU in compliance with the directive.

The Safe Harbor provides certain benefits, especially for U.S. vendors that deal with numerous entities in the EU. A single certification allows an organization to import personal data from multiple entities without having to enter into a "model contract" each time. However, in contrast to the "model contract," which is virtually risk free if done correctly, companies that self-certify to the Safe Harbor must renew their certifications each year. They also run the risk of an FTC enforcement action if they fail to do so correctly, or claim to be self-certified when they have forgotten to renew their certifications.

Perhaps of greater concern is increasing pressure from certain sectors within the EU that the Safe Harbor is a poor solution to the adequacy requirement, and should be eliminated, or at least re-evaluated. These criticisms have intensified in light of recent news reports of U.S. spying on EU residents. For example, in October, the European Parliament's Civil Liberties,

[5] Art. 6.1(c) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

Justice and Home Affairs (LIBE) committee assessed the Safe Harbor as part of its inquiry on "Electronic Mass Surveillance of EU Citizens." Testimony before the LIBE suggested that numerous companies are not in actual compliance with the Safe Harbor despite claiming so in their certification statements. There also were complaints that many companies do not provide a dispute resolution mechanism, or rely on the American Arbitration Association which — according to critics — is too expensive an avenue for most individuals to pursue.

Other EU officials and privacy advocates have suggested that the Safe Harbor be suspended as a sanction against U.S. surveillance activities. For example, Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship, recently stated "the existing scheme has been criticized by European industry and questioned by European citizens: They say it is little more than a patch providing a veil of legitimacy for the U.S. firms using it."[6] Back in July, Reding stated that the Safe Harbor was a "loophole" and that the European Commission would be undertaking a review of the Safe Harbor, with its assessment expected by year-end.

Practice Point

While the Safe Harbor may be amended at some point, there seems little chance that the Safe Harbor will be suspended or terminated, at least not without significant lead time for companies to transition away from it. Nonetheless, companies may want to take the following steps:

- If a company is relying on a data processor's Safe Harbor certification to transfer data from the EU to that company, its agreement with that processor should: (a) require the processor to provide immediate (and where possible, advance) notification if it is no longer certified or plans not to renew its certification and (b) require the processor to immediately enter into a model contract or binding corporate rules if it loses its certification or the Safe Harbor is terminated or suspended. This contract provision is a "best practice" even if the Safe Harbor remains untouched; and
- Companies that themselves rely on Safe Harbor certification for intracompany data transfers from the EU the U.S. should be aware of the growing concerns being voiced in the EU.

[6] *See* Viviane Reding, "Towards a More Dynamic Transatlantic Area of Growth and Investment" (Speech, Center for Transatlantic Relations, Oct. 29, 2013), *available at* http://europa.eu/rapid/press-release_SPEECH-13-867_en.htm?locale=en.