E-ALERT June 24, 2009

EU Data Protection Advisory Body Publishes Opinion on Online Social Networking

The Article 29 Working Party (WP 29), the influential EU data protection advisory body composed of national data protection authorities, published on June 19, 2009 an opinion analyzing how European data protection principles apply to social networking sites (SNS) (WP 163).[1] Data protection regulators in Europe have expressed several concerns in recent years regarding the regulation of SNS,[2] but this is the first time the WP 29 has released an opinion paper on the subject. While the WP 29 addresses some important issues -- such as access to user profiles and posting third-party information online -- it also reaches some surprising conclusions that are likely to trouble operators and users of SNS, as well as third party application providers.

Application of the Data Protection Directive

The WP 29's analysis of the application of the Data Protection Directive to SNS will be of interest and in some cases give cause for concern to many SNS providers.

Jurisdiction over SNS providers

The WP 29 concludes that SNS providers are subject to European data protection laws "in most cases, even if their headquarters are located outside of the EEA." The WP 29 relies on the fact that in these cases SNS providers are "making use of equipment" in the EU, and refers to an earlier WP 29 opinion paper concluding that jurisdiction over non-EU based website operators may exist where cookies are deployed onto the PCs of persons located in the EU.[3]

SNS provider and user as "data controller"

The WP 29, not surprisingly, concludes SNS providers, as well as potentially third-party application providers, are regulated as "data controllers" under European data protection laws. More surprisingly, the WP 29 concludes that SNS users can be data controllers as well (and not just data subjects). While acknowledging that European data privacy law exempts persons

[1] WP163, "Opinion 5/2009 on online social networking," adopted on June 12, 2009:t http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

[2] *See, for example,* the 'Rome Memorandum,' adopted in March 2008 by the Berlin International Working Group on Data Protection in Telecommunications, available at http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf, as well as the Resolution on Privacy Protection in Social Network Services, adopted on October 17, 2008 by the 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg, available at, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf

[3] WP148, "Opinion 1/2008 on data protection issues related to search engines," adopted on April 4, 2009: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf

COVINGTON
COVINGTON & BURLING LLP

BEIJING
BRUSSELS
LONDON
NEW YORK
SAN DIEGO
SAN FRANCISCO
SILICON VALLEY
WASHINGTON

WWW.COV.COM

using data for purely domestic or personal purposes, the WP 29 finds that this exemption may not apply where users "act on behalf of a company or association, or use the SNS mainly as a platform to advance commercial, political or charitable goals" or where they have a high number of third-party contacts that are unknown to the individual -- meaning such users could qualify as data controllers.

Default features of SNS service and sensitive data

The WP 29 states that SNS providers must ensure privacy-friendly default settings are in place, including settings that restrict access to user profiles to the user's own, self-selected contacts. The group also expects that service settings should require the user's affirmative consent before any profile data becomes accessible to other third parties, and that restricted access profiles should not be discoverable by internal search engines. Where users are asked to provide sensitive data in connection with their profile, they should be told that the data are optional. More generally, SNS providers may not process any sensitive data about SNS members or non-members without their explicit (i.e., free, informed and specific) consent.

Information SNS should provide

The WP 29 recommends that SNS providers (i) provide adequate warning to users about the privacy risks of the service, (ii) remind users that uploading information on third parties (e.g., "friends" or "contacts") could infringe their privacy, and (iii) advise users that they should seek the consent of third parties if they wish to upload pictures or content containing data about them.[4] The WP 29 also calls upon SNS providers to set up and refer to a "complaints handling office" on its website, which would deal with privacy-related issues and concerns.

Problematic practices: processing data of non-members

A few practices come in for particular criticism within WP 163. First, the WP 29 is clearly opposed to SNS providers constructing profiles of non-members using information provided by persons using the SNS service -- for marketing purposes or otherwise -- concluding that this "lacks a legal basis." Second, the use of sensitive user data to deliver targeted advertising appears to raise particular concerns for the group. Third, the retention of user data after a user leaves a service is questioned. Now, SNS providers will be expected to delete user profiles promptly once an account is de-activated, unless it is necessary to retain data to prevent identity theft or related crimes. Further, if a user fails to use the service for an extended period of time, the profile should revert to an inactive status.

The paper ends by discussing the status of children and minors, but only outlines a broader strategy that includes educational initiatives, privacy-enhancing technologies, age verification measures and similar tools.

Comment

The suggestion that certain users could be data controllers is likely to prove a highly contentious aspect of the opinion and will engender much uncertainty. This could mean that some users would have an obligation to register with European data protection authorities, apply security measures to "their" data, and comply with data transfer rules -- a conclusion that is likely to appear unworkable to many people. Increased obligations also could have unfortunate consequences for the burgeoning market in associated applications. This WP 29 opinion and some aspects of the analysis is bound to attract significant attention both in Europe and the US given the increasing use and importance of SNS to individuals and companies.

[4] WP 29 suggests that this could be made easier by introducing tagging management tools within social network websites, for example, by making available areas in a personal profile to indicate the presence of a user's name in tagged images or videos waiting for consent, or setting expiration times for tags that have not received consent by the tagged individual.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our global privacy & data security practice group:

Daniel Cooper	Erin Egan	Henriette Tielemans	Mark Young
+44.(0)20.7067.2020	202.662.5145	32.2.549.5252	+44.(0)20.7067.2101
dcooper@cov.com	eegan@cov.com	htielemans@cov.com	myoung@cov.com

This information is not intended as legal advice, which may often turn on specific facts. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP is one of the world's preeminent law firms known for handling sensitive and important client matters. This promotional communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts. Covington & Burling LLP is located at 265 Strand, London WC2R 1BH.
© 2009 Covington & Burling LLP. All rights reserved.