Non-EU websites face liability under EU data privacy laws

By Dan Cooper

DESPITE BEING LOCATED outside the European Union, non-EU website operators using cookie technology could find themselves being brought under the jurisdiction of the EU Data Protection Directive.

In a recent working document, the European Union's Article 29 Data Protection Working Party has given the clearest expression to date of its belief that the EU Data Protection Directive applies in full to certain online activities of businesses outside the EU (see note 1).

Organisations running websites that use so-called "cookies" and related devices that collect personally identifiable information on European Internet users now appear to be potentially liable for violating European data protection laws, despite having no legal or physical presence in the EU. Although the full impact of this development remains to be seen, it will certainly come as an unwelcome surprise to website operators who have historically regarded themselves to be safely beyond the reach of Europe's privacy laws.

These organisations would be wise to regard the Working Party's document as a regulatory shot fired across their bows, and to consider their compliance options sooner rather than later.

THE "COOKIES" THEORY

The Working Party's paper generally reflects a longstanding concern with the "international application of EU data protection law to the processing and – in particular – collection of personal data by websites which are based outside the European Union" (Working Document, p.2). The Working Party's specific attention, however, is devoted to organisations that deploy cookies, JavaScript and, less commonly, parasitic "spyware" applications to gather and process personal data about European Internet users.

In assessing whether these organisations need to ensure that their conduct conforms with the EU's Data Protection Directive, the Working Party logically turns to the Directive's national law provisions contained in Article 4.1(c).

ARTICLE 4.1(C)

Article 4.1(c) provides that EU Member States shall apply their national data protection laws to an organisation, or data controller, even when it is not established in the EU, provided that the organisation:

> "**makes use of** equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit..."
>
> **– Article 4.1(c), EU Data Protection Directive**

This begs the next question: does an organisation situated outside the EU, but operating a website available to European Internet users, "make use of equipment" inside the EU?

The Working Party has just answered: "yes". It adopts an interpretation of the phrase, "makes use of", which it suggests (an opinion not unanimously shared) reflects the emerging jurisdictional principles of international law in the online environment. According to the Working Party, in order to "make use of" equipment in the EU, an organisation need only exercise limited control over the functioning of the equipment. Put another way, an organisation makes use of equipment so long as the equipment remains at its "disposal" for purposes of processing data (Working Document, p.10). The Working Party rejects the view that an organisation must enjoy ownership interest in the equipment, partial or otherwise, or exercise complete control. And, as it reveals in the context of cookies, the organisation need not even determine the fact, or time and place, of the equipment's use.

The Working Party does concede that the organisation should be guiding the "relevant decisions" concerning both the substance of the data collected and the nature of its processing by means of the equipment. Whether, and to what degree, other parties can divest the organisation of effective control by contributing to the making of the "relevant decisions" remains an open question (see note 2).

COOKIES, JAVASCRIPT & SPYWARE

The Working Party, armed with its interpretation of the phrase "makes use of", turns to the deployment of cookies, JavaScript and spyware by website operators outside the EU. It concludes that those devices enable organisations to control (in the Article 4.1(c) sense) the personal computers of European Internet users. Thus, when these organisations collect and process personally identifying data about an Internet user they are subject to the directive. Specifically, they are subject to the data protection law of the Member State in which the Internet user's computer is located.

Given the absence of any actual physical presence in the EU, the Working Party instructs these organisations to appoint a representative in the relevant European jurisdiction in accordance with Article 4.2 of the Directive (see note 3).

By way of example, imagine a Canadian business that owns and operates a website that places cookies onto the computers of its visitors to improve functionality and facilitate access. A Spanish Internet user visits the Canadian website, volunteers his name and address, but also has a cookie placed on his computer hard drive. On the Working Party's jurisdictional theory, the Canadian business may find itself liable for failing to ensure that its data processing activities conform to Spanish data protection law.

Most probably, it has violated the law by failing to notify Spanish data protection authorities of its data processing activities. It may also have failed to address related obligations such as furnishing adequate notice to European visitors to the site, legitimising its data processing activities and complying in full with subject access requests. Because users from all 15 Member States will visit the website, the Canadian business must contemplate compliance with 15 separate European data protection regimes.

The Working Party's jurisdictional theory gives rise to at least three observations.

First, it plainly accepts that not every exchange involving a European Internet user and a website located outside the EU will trigger the application of EU data protection laws, and the critical element of control will be absent where cookies and similar devices are not deployed. By bringing non-EU businesses that use cookies and JavaScript within the ambit of European data protection laws, European regulators provide a real incentive for such businesses to limit their use of cookies and JavaScript, and offer European Internet users only the most bare-boned, non-interactive web browsing experience.

Privacy advocates may view this as a small price to pay to ensure adequate protections exist for any personal data obtained by such businesses, but consumers may disagree.

> ...the Working Party does not view all cookies as equal, and some are more troublesome than others.

Second, the Working Party does not view all cookies as equal, and some are more troublesome than others. Control over a European Internet user's computer is more likely to occur when website operators utilise persistent cookies – those that reside on an Internet user's hard-drive after their web browsing session has concluded – as opposed to session-based cookies that are deleted at the end of the website session. Similarly, third-party cookies delivered indirectly onto the Internet user's computer, such as those commonly employed by cybermarketers and Internet advertisers to deliver banner ads, are more problematic from a privacy perspective than first-party cookies placed directly from the website that has been visited. Consequently, businesses whose websites deploy persistent, third-party cookies remain considerably more exposed to liability than business using first-party, session-based cookies.

Third, the Working Party's paper raises the interesting possibility that control can be transferred to the Internet user, eliminating jurisdiction. Website operators theoretically should be able to abdicate control over an Internet user's computer in favour of the user. What this might require in actual practice is not entirely clear, and the Working Party offers no guidance. For instance, does a business relinquish control by notifying Internet users of its cookie policy, by offering visitors the opportunity accept or decline the cookie with a prompt box, or by enabling visitors to tailor the cookie to suit their particular wishes before accepting it? Or, will some members of the Working Party continue to regard certain cookies, such as persistent third-party cookies, as inherently controlling, no matter how they are presented to the Internet user?

Alternatively, control conceivably could be lost as Internet users increasingly take advantage of privacy-enhancing technologies to manage cookie-type applications, including "cookie killer" web browsers and cookie taming software (for example, cookie washers, cookie cutters, and cookie crunchers).

CONCLUSION

It remains too early to tell what the consequences of the Working Party's latest document will be, and whether it is a sign of enforcement activity to come. Certainly, some businesses will adopt a wait-and-see approach, delaying compliance as late as possible or until website operators are prosecuted, if ever.

They may, rightly or wrongly, view the enforcement risk to be slight given the nature of their data processing, consider themselves to be judgment proof because they lack any meaningful presence in the EU, or regard the chances of recognition and enforcement by a domestic court of an adverse foreign judgment to be slight.

This strategy could prove short-sighted, however, and ignore the possibility that the organisation may later need to acquire a European presence or underestimate the public-relations consequences of even an unsuccessful prosecution for privacy violations.

Moreover, if such an organisation is successfully prosecuted, its knowing disregard of the law may result in harsher sanctions than had the business sought to comply with European laws in the first place.

For many organisations, the reduction or elimination of any potential liability under European privacy laws may prove to be the more prudent course. Some organisations may want to seriously consider modifying their websites in an effort to remove themselves from EU jurisdiction under the Working Party's new theory. Such organisations will have to weigh up options such as removing or amending their policies regarding cookies, JavaScript and spyware, eliminating any persistent or third-party cookies, seeking clear consents before placing devices onto an Internet user's computer, and differentiating the treatment of European Internet users from others. Alternatively, some organisations might reasonably conclude that they can only reduce their exposure by complying with European data protection laws, and begin to consider ways to address this fact. These organisations will need to address squarely all the compliance issues that currently confront businesses already established in the EU.

Although an organisation's optimal approach will depend on its unique circumstances, all organisations potentially at risk would be well advised to make an educated assessment of their situation, evaluate their options, and select an appropriate and informed compliance strategy before it proves to be too late.

Dan Cooper, is Senior Associate at law firm, Covington & Burling. He can be contacted by e-mail at: dcooper@cov.com

Notes:

1. Article 29 Data Protection Working Party - Working document on determining the international application of EU data protection law to personal data on the Internet by non-EU based websites, WP 56, 5035/01/EN/Final, 30 May 2002. See: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

2. The Working Party deems their interpretation to reflect a "cautious approach," presumably on the basis that Article 4.1(c) on its face only requires the mere use of equipment in the EU, without stating more (Working Document, p. 10). The Working Party's position is likely a reflection of not simply caution, but an underlying appreciation that a broader interpretation could lead to difficulties with enforcement and recognition by non-EU courts.

3. Article 4.2 of the directive provides that: "In the circumstances referred to in paragraph [4.]1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions, which could be initiated against the controller himself." The Working Party also suggests that a single representative could serve as a representative agent on behalf of more than one organisation.

A PL&B short guide to cookies

WHAT ARE COOKIES?

Cookies are small text files placed on Internet users' web browsers when they access certain websites. Basically, cookies are used to send information back and forth between web servers and users' computers.

WHAT ARE THE BENEFITS?

Cookies can enhance a user's web browsing experience. They can be used to personalise web content by building up a profile of a consumer's preferences. They can store online ID information, allowing consumers to use online shopping carts and access familiar websites without having to key in their details with each visit.

WHAT ARE THE PRIVACY RISKS?

Cookies that store users' ID and password information could pose a security and privacy threat if the computer is shared with other people, for example, in the workplace or a cyber cafe.

Cookies can be used to build profiles of individuals' web browsing habits, more often than not, without their knowledge or consent.

Generally, the information is processed anonymously, but there is concern that some organisations have sought to link such data with personally identifiable information.

SESSION COOKIES

A sesssion cookie will gather data only for the duration of a user's visit to a particular website. These cookies are deleted from the user's web browser once the website session is terminated.

PERSISTENT COOKIES

Persistent cookies are stored onto users' hard drives and can remain for an indefinite period, sometimes years. They can be used to facilitate online shopping (shopping carts), pre-filled registration forms, or personalised web pages.