PRYOR CASHMAN LLP

LEGAL UPDATE

November 2010 *By: Jeffrey C. Johnson and Donata von Gruben*

INTERNET PRIVACY POLICIES AND THE EU

Unlike the "brick and mortar" world, the Internet operates without geographic restrictions and knows no borders. As a result, US-based operators of websites cannot simply ignore the laws and regulations of other jurisdictions. This is particularly true in respect of the European Union because it is one of the largest unified markets outside the US. In recent months, this fact has been highlighted by the increasingly high-profile issue of privacy protection over the Internet, an area where the EU has been far more aggressive with regulatory oversight than in the US

Indeed, compliance with EU regulations governing privacy in the on-line world is a concern not just for companies having their offices or substantial operations in the EU, but also for businesses that may be located, and primarily operate, in the US and other third countries, but that use the Internet to serve customers located in the EU. According to Article 25 of Directive 95/46/EC, the EU-wide regulation from which national privacy protection laws of EU member states stem, the transfer of personal data to a country outside the European Economic Area (i.e., the EU plus a few additional states that participate in the economy of the EU without being formal member states of the EU) is generally prohibited unless there is an adequate level of protection for personal data in that country. In large part due to the *laissez faire* approach of US regulators to Internet privacy, the European Commission and European regulators take the view that the US does not provide adequate protection for personal data.

Under EU regulations, "Personal data" generally means data concerning individuals and which enables the direct or indirect identification of those individuals. The understanding of the term "personal data" as used in the EU directive however is, by US standards, very broad; it includes not only direct "identifying information" (e.g., names and addresses), but also much of what is commonly referred to as "Anonymous Information". For example, even though it can't be directly associated with a particular natural person, an IP Address is considered as being personal data under the EU directive, and therefore must be processed in accordance with the EU regulations. Hence, privacy regulation in Europe concerns every US company that has an interactive Internet presence within the EU.[1]

Consequences of breach of EU privacy regulations may range from injunctions (i.e., prohibiting the company from engaging in the prohibited conduct), fines and compensatory damages to criminal sanctions including imprisonment, depending on the severity of the violation of law and the laws of the particular EU member state where the violation has taken place. Monetary penalties can be as high as several hundred thousands Euros. A recent proceeding against Google in Italy, where three Google executives were convicted by an Italian court for allowing a video of a teenager with Down's Syndrome being bullied by other teenagers to remain online for two months, demonstrates how serious the consequences of non-compliance of EU regulations can be: each executive was given a six-month suspended sentence for violation of privacy.

To date there have only been sporadic, relatively limited efforts to enforce EU privacy regulations against American companies, but this issue gains more and more relevance as the development of digital technology – data processing , data capture, data storage, data transfer and data analysis –

[1] And arguably even those who screen out users located in the EU, since in order to screen out a user, the website operator must collect the IP address of that user.

continues to widen the gap between users' privacy expectations and the information that can in fact be garnered from a person's use of the Internet. Privacy groups in the EU therefore increasingly not only deal with the fundamental questions of how data is protected on the Internet, but also with the effective enforcement of users' privacy rights. To minimize the risk of running afoul of EU regulations and becoming an example for EU efforts to more aggressively enforce those regulation, website operators based in the US should consider two alternative solutions:

MODEL CONTRACT CLAUSES:

The European Commission provides standard form contracts which can be entered into between US entities and their affiliates based in the E.U. (including affiliates organized expressly for this purpose). The EU-based affiliate is the formal owner of the relevant data, and agrees to make that data available to its US affiliate subject to restrictions on the use of the data that are equivalent to the statutory restrictions under EU law. According to the privacy protection regulations of the various EU member states, the transfer of data to the US ordinarily needs to be approved by the respective regulating authorities, which consider whether the level of data protection corresponds with the level of protection stipulated by the EU. The benefit of the model clauses is that they effectively constitute a substitute for the EU member state's approval because those member states are bound by the decisions of the EU Commission (the body responsible, among other things, for proposing and implementing EU regulations), which has concluded that the model contract clauses provide the appropriate level of privacy protection. The model contract also grants users a right to enforce the model contract clauses addressing the obligations of the parties to protect the privacy of users. The model contract clause were last amended in May 2010 in an attempt to better conform to actual practice in light of the fast pace of change in international commerce. Compliance with the model contract clauses is enforced by the regulating authorities of the various EU member states.

SAFE HARBOR (http://www.export.gov/safeharbor/):

An exception to the rule that the US does not provide an adequate level of data protection is made where companies voluntarily register with what is known as the Safe Harbor program. This is a framework to bridge the different privacy approaches between the EU and the US It involves certifying on a public register that the company will abide by Safe Harbor principles. These principles again are broadly equivalent to the EU privacy protection regime. The Safe Harbor alternative is only available for companies that are regulated by the Federal Trade Commission. Large public companies, such as Google Inc., Bertelsmann Inc., Deloitte LLP, Ernst & Young LLP, Johnson and Johnson and Facebook Inc., and more than 2000 other companies independent of size and field of activity, have already registered with Safe Harbor program. Enforcement against registered companies is the responsibility of the FTC; however enforcement actions brought by the FTC under the Safe Harbor program are very rare.

Unlike the US, the EU and its member states have developed a much more aggressive regulatory regime for protecting the privacy of Internet users. Generally, any operator of a website based in the US will run afoul of that regulatory regime if the websites functionality has any interactive components that are accessible to users residing in the EU. Website operators that have not already taken steps to bring themselves into compliance with EU requirements for privacy protection should be evaluating their business to determine whether they receive and store personal information provided by those users and, if so, how they might ensure compliance with the EU's requirements.

***

The foregoing is merely a discussion regarding internet privacy policies and the EU. If you would like to learn more about this topic or how Pryor Cashman LLP can serve your legal needs, please contact Jeffrey C. Johnson 212-326-0118.

About the Author

Jeffrey C. Johnson
Partner

Direct Tel: 212-326-0118
Direct Fax: 212-798-6314
jjohnson@pryorcashman.com

Jeffrey Johnson is a partner specializing in the transactional aspects of technology and intellectual property exploitation (patents, trade secrets, trademarks and copyright) including, in particular, all aspects of mergers and acquisitions, joint ventures, strategic alliances, private placements and licensing in the biotech, entertainment, Internet, pharmaceutical, software and telecommunications industries.

Jeffrey typically focuses on transactional matters principally involving intellectual property or goods and services the value of which is largely attributable to intellectual property. He has represented, among others:

- A public biotechnology company negotiating and documenting numerous strategic alliances, research and development collaborations, co-promotion agreements, patent and know-how licenses, and other agreements relating to the development and exploitation of the company's core technologies
- A public telecommunications company in connection with a strategic reorganization to maximize the value of its patent portfolio and licensed rights
- A private equity fund in connection with the acquisition and disposition of patent portfolios
- A pharmaceutical company's bioinformatics group negotiating and documenting numerous strategic alliances, software development agreements and software licenses, as well as the group's form agreements for the provision of bioinformatics services and the licensing of genomic and proteomic databases
- A technology-transfer company in connection with the sale of a portfolio of patents governing web-enabled software updating, active desktop and offline browsing
- A Korean cell phone manufacturer in connection with the negotiation and documentation of a hand-set supply agreement with large, U.S.-based cell phone service provider
- A telecommunications company in connection with its sponsored research agreements with various U.S. and foreign educational institutions
- A health services company in connection with the purchase of an information management business including a large, proprietary prescription drug database
- A European-based public company in connection with the negotiation and documentation of a strategic alliance providing for the joint development and commercialization of an ASP-based software application useful for the on-line calculation, reporting and remittance of sales tax obligations
- A public pharmaceutical company in connection with the disposition of certain patent portfolios and related clinical data and know-how useful in connection with small molecule anti-genomic therapeutics and small molecule anti-bacterial therapeutics
- A privately held company in connection with the sale of a portfolio of patents governing "Web 2.0" search methodologies
- A public biotechnology company in connection with the negotiation and documentation of agreements providing for the further clinical development and commercialization of a Phase I pharmaceutical compound in collaboration with a Fortune 100 pharmaceutical company, including a license agreement, a co-promotion agreement and a manufacturing and supply agreement

Jeffrey has been an invited speaker and panelist at a variety of public and private events.