The European Union ("EU") regards the United States ("US") as being "inadequate" when it comes to data protection. Europeans tend to take this at face value and presume that there must be a good reason why the European Commission has come to such a radical conclusion. Americans, naturally enough, tend to take unkindly to being told they are inadequate, particularly when it implies that their democracy has failed to protect a fundamental right, like the right to privacy. So are the two jurisdictions as diametrically opposed as they are portrayed?

**Contrasting Perspectives**

There is relatively little probing debate about the legitimacy of the EU’s view of US data protection laws. Instead, the high level debate in the EU tends to comprise fairly generic references to the US not having a "culture" of privacy, the bemoaning of any US federal data protection laws and an underlying suspicion that the US PATRIOT Act and other US security and anti-terror legislation is being used in a manner that tramples on the privacy rights of any person who has their data processed on a US server.

For its part, the US perspective often focuses on the existence of sector-specific privacy laws in the US, the vagueness of the EU data protection principles and their practical impact on the free movement of data and therefore on innovation and commerce.

US multinationals also point to the fragmented approach to the interpretation and enforcement of the existing EU Data Protection Directive across the EU’s 28 Member States.

The contrast in the views of the two sides were captured succinctly in a recent New York Times article which featured the following quote from Cameron F. Kerry, General Counsel of the US Commerce Department:

"The sum of the parts of US privacy protection is equal to or greater than the single whole of Europe."

The next paragraph of the same article contained a quote from Peter Hustinx, the EU Data Protection Supervisor:

"Yes, we share the basic idea of privacy. But there is a huge deficit on the US side."

**Trade Implications**

This underlying distrust between the two sides manifests itself regularly, for example in the case of the transfer of passenger name records to the US from European airlines, Google’s ability to change its Privacy Policy on a global basis and, most recently, in the debate about the proposed EU Data Protection Regulation. On a broader economic level, the differences between EU and US privacy laws are being quoted as...
Google Auto-Complete and the Frontier of Individual Privacy Rights in Germany

By Dr. Markus Bauer, Partner, Rittershaus

In its decision of May 14, 2013 Germany’s highest court, the Federal Court of Justice, significantly expanded the rights of individuals to have potentially libelous or defamatory results removed from the suggestions provided by Google’s auto complete function in the Google search bar. This decision may set new standards for search engines and its implementation may be quite costly for Google.

Imagine you are the owner of an online cosmetics retailer and when your name is typed into Google’s search bar the auto complete function suggests the terms “Scientology” and “Fraud” as additional search parameters. Or you are the wife of the president of Germany and the search suggestions in connection with your name are “Prostitute” and “Escort Lady”. In both cases the persons affected have taken Google to court and the first case has now been decided by the Federal Court of Justice in favor of the complainant, overturning decisions by both the District Court and the Court of Appeals in Cologne.

Google’s main argument, which was upheld by the two lower courts, was that the suggestions made by the auto complete function are based on an algorism which automatically analyses the terms searched by other Google users in connection with the complainant’s name. In this case the suggestions were based on respective (unfounded) rumors exploited by Germany’s tabloids. This is simply an additional feature designed to make a specific search easier and faster for Google users and the suggested terms could in no way be interpreted as being Google’s own proposal based on any kind of sensible criteria or the provisions of links or other access to respective opinions of third parties.

Following, to a large extent, Google’s arguments, the court of appeals in Cologne held that the suggestions made by Google auto-complete only contain the statement that other Google users previously searched this particular combination of keywords. This is a true statement of facts which does not constitute any violation of privacy rights.

This position, which is consistent with pervious judgments of other German court in particular with respect to snippets presented as search results, was then rejected by the Federal Court of Justice in its decision dated May 14, 2013. Even though, the full text of the decision has not yet been published, the extensive press release provides a reasonably good insight into the court’s reasoning. Following the plaintiffs arguments, the court held that even though the suggestions by Google’s auto complete function were created automatically solely based on search terms most frequently used by other Google users in conjunction with the relevant name, these suggestions “contain an ascertainable statement by Google that there exist a connection between the person whose name is searched and – in the case at hand – the terms “Scientology” and/or “Fraud” which have a negative connotation”. Depending on the gravity of this negative connotation such statement, if it is untrue or unsubstantiated, may constitute a violation of the privacy rights of the individual concerned and provides injunctive relief.

As a result Google does not have to automatically screen all auto-complete suggestions but once it has been notified of potentially libelous terms being suggested it must remove this suggestion from its database and if it

Subject to the analysis of the full decision which is yet to be published, this case seems to be a deviation of the previous position of German courts in relation to search engines and a significant expansion of individual privacy rights. The Federal Court of justice now seems to apply the responsibility of host providers pursuant to section 10 German Telemedia Act analogous to search engines and it will be interesting to see how the scope of such responsibility is further defined in future decisions.
California’s Right to Know Act of 2013 Seeks to Enhance Transparency as to Personal Data Uses

By Aldo M. Leiva, Founder, Leiva Law, P.A.

California has led the U.S. in the development of privacy protection law and a new California law, entitled the “Right to Know Act of 2013,” (AB 1291) seeks to further extend consumer privacy rights by allowing for greater transparency as to disclosure of personal consumer information by businesses and incorporating privacy protections similar to those provided under European Union (EU) law. Under current California law (section 1798.83 of California Civil Code), businesses that collect consumer information and disclose said information to third parties for marketing purposes must notify consumers of any third party recipients of said information, upon request by consumers. All such information is provided free of charge. Businesses are also required to ensure the privacy of consumer personal information by adopting measures to destroy such records. Further, businesses must disclose privacy policies to consumers and provide designated means of preventing disclosure of such information. Consumers may sue for statutory violations under the existing law, and may recover damages or seek other relief, including injunctive relief.

The proposed Right to Know Act of 2013 would amend existing law by requiring that businesses that retain customers’ personal information or disclose said information to a third party, would be required to provide, at no charge and within 30 days of written request, (1) a copy of disclosed information and (2) names and contact information for all third parties to whom such information was disclosed within the last 12 months, to a customer within thirty days of a request. Such information would be provided at no charge and would be provided regardless of whether the business has a relationship with the requesting individual.

The bill’s definition of “personal information” includes names, social security numbers, and birthdates, and can also include a user’s IP address, mobile device data and geolocation data. Although the proposed legislation further expands disclosure duties of businesses as to personal information, it sets no limits on the amount of data that can be collected, nor does it limit how such data is secured or with whom it can be shared. However, as drafted, the legislation would have the practical effect of requiring businesses to offset the costs of compliance with personal information requests, such as increasing costs of services or products. Similarly, expanded compliance requirements may require updates to data storage and retrieval systems to facilitate data search and disclosure.

Privacy advocates have supported the bill as a foundational step in educating consumers as to how personal data is being utilized and empowering them in deciding on whether to continue relationships with businesses that retain their personal information.

“… a foundational step in educating consumers as to how personal data is being utilized and empowering them in deciding on whether to continue relationships with businesses that retain their personal information.”

Privacy, E-Commerce & Data Security Committee - Quarterly Newsletter
The BYOD Trend – The Use of Personal Devices in the Workplace

By Renato Opice Blum, Attorney, Economist and President of the IT Advisory Board of Fecomercio

The time has gone when those with access to cutting edge technology was limited to individuals working in enterprise environments. Today, information is freely available about the quality, robustness and efficiency of products, enabling ordinary users to receive and track news of what the domestic or international electronics market has to offer. On the other hand, many companies still operate more traditional forms of supply acquisition, with all the usual bureaucracy and delays. This, combined with volatile budget policies, leads to a tendency for a decrease in the pace of technological modernization in the workplace.

An increasing reality in Brazil is employees often prefer to use their own devices, which are more modern and versatile, to conduct their activities rather than use devices offered by their employer. In this context, managers may choose to cautiously take advantage of the model, known as Bring Your Own Device (BYOD). As with many other day to day facts of life, this partnership between worker and employer can be productive, however the following precautions should be considered and adhered to.

First, the risks involved and the terms of art. 2 of Consolidacao das Leis do Trabalho (Consolidation of Labor Laws), the company must define which activities may be carried out on the employees' private equipment. Similarly, the employee should understand the necessity to use original software, tools and adequate security configurations as failure to do so would leave the company infrastructure vulnerable.

Thus, where a company recognizes, for its security, that personal equipment with access to its systems should be verified, it must be recognized that there is no legal provision or consolidated jurisprudence on this point. Therefore, it is essential that the employer expressly negotiate, clarify and formalize this situation with its employees. This can be accomplished in a specific document laying out the settings and conditions that must be applied if any technological equipment is used. Moreover, during this process, standards and minimum configurations can be set to grant access to the systems, whilst also demanding periodic verification that the employee is continuing to meet these requirements.

It is also important to clarify the working hours of employees prior to the adoption of the BYOD model. It is a good idea to set timetables and to limit the availability of the worker through their devices, as, the use of their private device, should not necessarily be considered as overtime or being on duty.

To summarize, the principles governing this new facet of the employment relationship may be those that, not contrary to the law, create interesting situations for the parties, demonstrating the free and conscious choice of each to assume the risks of the proposal whilst avoiding the potential for future trouble. The equilibrium of work relationships, whatever the case, should always be preserved as we can have little doubt as to what side the law is most likely to favor.

It is essential that each party understands from the outset their own responsibilities. An issue of some considerable controversy revolves around interference, by employers, into the equipment of its employees and the monitoring of such equipment. It is important to note that, currently, there are no firm precedents regarding the legality of monitoring employees own equipment, especially as it may contain their private content, the manipulation of which could prove highly problematic.

To keep up with all PEDS related news, publications and events, check out the PEDS Committee website!

http://apps.americanbar.org/dch/committee.cfm?com=IC736000
as one of the major stumbling blocks to the current EU-US negotiations on a far-reaching trade and investment partnership agreement known as TTIP (Transatlantic Trade and Investment Partnership).

On closer examination however, two of the world’s biggest trading blocs are not as far apart as they sometimes seem when it comes to the regulation and protection of data.

**Data Security Laws**

Looked at objectively, US data security laws are more developed than those in the EU. While the EU relies upon a broad principle of “adequate security” in the Data Protection Directive, the US has at least 30 acts of Congress that address the issue of information-based security with more than 40 Bills and Resolutions relating to cyber-security proposed in the recent 112th Congress. The US legislative framework is complex as it lacks an overarching cyber-security framework law with the law instead enshrined in many different federal and non-federal laws addressing various aspects of cyber-security. These extensive measures are rarely acknowledged in the EU debate about US adequacy.

In addition, the US has various Executive Branch actions, such as the George W. Bush Administration’s “Comprehensive National Cybersecurity Initiative” which was established by Presidential Directive in 2008. However, the contents of that initiative are classified, which does little to quell EU distrust. The recent Prism controversy has raised the temperature in the debate between privacy advocates and those favoring extensive monitoring in the context of law enforcement.

**Data Breach Notification Laws**

In the EU, mandatory data breach reporting is currently restricted to those in the communications industry under the ePrivacy Directive 2002/58/EC, although this is proposed to extend to all sectors if the proposed Data Protection Regulation is adopted.

In the US, 46 States already have laws requiring notification of security breaches involving personal information (California was the first State to do so in 2002) while various federal statutes, regulations and memoranda require certain sectors (healthcare, financial, federal public sector and the Department of Veteran Affairs) to also report breaches.

**Lawful Access**

The United States have many laws governing lawful access to data. When viewed from abroad, a lot is made of the fact that lawful access to emails older than 180 days old is easier within the US as it can occur without judicial involvement on foot of a subpoena issued by a state prosecutor. This lacuna is put down to the fact that the Electronic Communications Privacy Act was enacted in 1986 before the emergence of universal email systems. Various proposals have been put forward to update the regime since.

In the EU, the Data Retention Directive (2006/24/EC) aims to protect email and Internet content and the ePrivacy Directive also restricts the ability of communications providers to retain and access location data and traffic data. [FOOTNOTE: As recently as 24 June 2013, the EU Commission adopted a further Regulation on the measures applicable to the notification of personal data breaches under ePrivacy Directive which is due to enter into force on 25 August 2013 and aims to harmonise the notification of data breaches by telecommunications companies and internet service providers.]

However, notwithstanding these Directives, all EU Member States have their own national regimes governing lawful access to data in the context of criminal investigations, matters of national security etc. Notably, the proposed EU data protection reform package includes a specific proposal for a further Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

See, EU v US Data Protection, page 6
US v EU Data Protection

In other words, both the US and the EU espouse Internet freedom but both regimes include wiretapping/eavesdropping /lawful access laws (usually subject to judicial oversight) which mean that there are no absolute rights to privacy in either jurisdiction.

A Privacy Bill of Rights

In February 2012, President Obama announced a Consumer Privacy Bill of Rights which espoused principles which will be familiar to those who follow EU data protection. For example, principles such as transparency, respect of context (akin to “purpose limitation” in the EU), data security, rights of access and rectification, limits on data collection and accountability were put forward on grounds that American citizens were entitled to higher standards of privacy than currently exist. However, while the Bill of Rights was welcomed by EU Commissioner for Fundamental Rights and Citizenship, Viviane Reding, it has been described as moving at “a glacial pace” since. 5

A number of questions arise if the US was to adopt such a Bill of Rights. Would this be sufficient to overcome the EU reservations on US adequacy? If the answer is no, then is the EU position based on a minimum requirement for a more substantive federal US privacy law? If a minimum requirement is a federal privacy law, would this serve to materially improve the protection of privacy or would it serve only to create a baseline for a new breed of class actions across the US?

Conclusion

Outside of the EU, many countries, for example in Latin America, have recently adopted EU-style privacy laws, no doubt in an effort to improve trade relations with the EU, while nobody has followed the US model. This does not mean however that one model is necessarily superior to the other. The truth is that neither the EU nor US privacy regimes can be presented in absolute terms and any attempts to try to reconcile the two are probably futile.

Often referred to as a patchwork quilt, the US approach is inherently complex. It has focused predominantly on data security and on sector-specific privacy laws with enforcement by the Federal Trade Commission. Rather than get buried in the detail of these laws, a lazier narrative tends to be presented within the EU alleging, usually in absolute terms, that the US does not have “adequate” data protection laws. However, the truth is that both trading blocs have a lot in common when it comes to privacy regulation and both have their own inadequacies. Unfortunately, progress in bringing the sides together will continue to be hampered as long as there is a failure to understand and respect the legislative positions adopted on each side of the Atlantic Ocean.

The views expressed above are the personal views of an Irish data protection lawyer who does not claim to be a specialist in US law. With this in mind, any feedback or comments from PEDS Committee members would be welcome.

Endnotes:

1 Save in the case of companies who come within Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbor privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce.
4 e.g. the Electronic Communications Privacy Act, Stored Communications Act, Foreign Intelligence Surveillance Act.

Monthly Committee Conference Calls

Get more involved! Join the PEDS Committee’s monthly conference calls. The calls occur the first Thursday of every month at 11:00 am Eastern Time (GMT -5) or 3:00 pm GMT. The next call will take place on September 5, 2013. We will circulate the call in details to the listserv shortly.
German Regional Court Rules Apple's Privacy Policy Non-Compliant

By Anika Keswani, Senior Escalation Manager - EMEA, salesforce.com GmbH

A regional German court in Berlin has ruled that even though personal information is not collected by a branch Apple office in Germany, Apple’s privacy policy is not compliant with German data protection laws. Under the German law, Apple must reveal to customers specifically what their data will be used for – a general, global consent to usage of personal data is unacceptable. (Tung, 2013)

Though it is likely that Apple will appeal the decision, they may also revise their global privacy policy to accommodate these requirements. Alternately, they can develop a new policy specific to Germany. The case was brought by a consumer group – the Verbraucherzentrale Bundesverband (VZBV), or Federation of German Consumer Associations. Gerd Billen, the organization’s executive director, commented that the verdict “shows the importance of privacy for consumers in the digital world.” (VZBV, 2013)

Apple Found Guilty of Conspiring to Fix E-Book Prices

By Katherine Woodcock, Senior Associate, Lorenz

In more Apple news, on July 10, 2013, the U.S. District Court of the Southern District of New York has found Apple guilty of conspiring to fix the prices of e-books. The Court found that Apple, threatened by Amazon’s dominance of the e-book market prior to the release of the iPad in 2010, conspired with major publishers to fix e-book prices:

… the Publisher Defendants conspired with each other to eliminate retail price competition in order to raise e-book prices, and that Apple played a central role in facilitating and executing that conspiracy. Without Apple’s orchestration of this conspiracy, it would not have succeeded as it did in the Spring of 2010.

You can find the full text of the decision at www.nysd.uscourts.gov/cases/show.php?db=special&id=306.

Committee News

CyberSecurity Report and Resolution

The ABA Cybersecurity Task Force is preparing a draft Report and Resolution relating to unauthorized or illegal intrusions by foreign and domestic governments of computer networks utilized by lawyers and law firms. If you are interested in contributing comments, please contact either of our co-chairs.
Committee News, continued

PEDS Committee Business Plan

We are working on ideas for our Committee Business Plan for 2013/2014. If you would like to take on an active role in our committee in the coming year, please contact either of our co-chairs.

SWOT Analysis

The ABA is conducting a SWOT analysis (strength/weakness/opportunity/threat) in relation of the ABA’s international operations as part of the review by the Association’s Task Force on the ABA’s International Role. If you are interested in contributing comments, please contact either of our co-chairs.

Deadline for 2014 Spring Meeting Proposals

We are pleased to announce a change in the way we will be selecting programs for our future season meetings. Anyone with an idea for a program should communicate those ideas to Rob Corbet (rob.corbet@authurcox.com) and Katherine Woodcock (katherinewoodcock@hotmail.com) by the close of business on Wednesday, July 24, 2013. The Committee’s officers will then evaluate these proposals, combine where necessary, and work to formulate from 1-5 programs. It is not necessary that you submit slates of speakers but you should indicate your interest in the program and sufficient detail to explain it. Once the programs are approved by the Committee or group of committees in the case of joint programs, the committees shall designate a program chair for each program to submit the program. At the end of the process, the seasonal meeting co-chairs will be able to select the programs that the committees and their members have jointly decided are the ones they want.

If you have any particular difficulty in communicating with the relevant committee co-chairs, you are free to contact Steven Richman, Program Officer (smrichman@duanemorris.com), Jessica Smith, Senior Meeting Planner (Jessica-Smith@americanbar.org), the 2014 Spring Meeting Co-Chairs, or the program team and we will assist.

We look forward to reviewing the program proposals and to seeing you at the 2014 Spring Meeting!