ABA Section of International Law
Your Gateway to International Practice

Volume 2, Issue 2
Fall 2014

Privacy, E-Commerce & Data Security Committee
Quarterly Newsletter

INSIDE THIS ISSUE:

U.S. and E.U. Regulatory Conflict and Cloud Data Protection

Jennifer L. Mozwecz, Partner, Shams, Rodriguez & Mozwecz, P.C.

The discovery of the United States National Security Agency's (NSA's) spying on private citizens of the European Union, most notably German Chancellor Angela Merkel, has caused significant strain in the U.S.'s relationship with the E.U. regarding data security and privacy. However, it has brought into focus the larger question of how secure a person's information really is, who has access to such data, and who decides what criteria for handling such data is acceptable? In a time where data is collected, transmitted and stored among countless locations, determining how to effectively and legally monitor and regulate these activities is an ongoing debate.

The EU adopted the Data Protection Directive in 1995 which regulated the processing of data within the European Union (Directive 95/46/EC). However, the implementation of this directive on the national level resulted in 28 different and often conflicting national laws. For example, last year in the cases of *Secretary of State for Health and others v Servier Laboratories Ltd and others* and *National Grid Electricity Transmission plc v ABB Ltd and others,* the English court decided that documents stored in France must be disclosed in litigation, even though such disclosure risked prosecution under French law. Thus, companies who collect data may risk prosecution under the local laws of an EU member state in which they were not even aware such data was stored. This lack of standardized policies lead to the proposal of the EU General Data Protection Regulation in 2012 which may come into effect next year, and requires that data controllers (those entities owning data) and data processors (those hosting data) share liability for data breaches and violations of the law under the new cohesive regulatory scheme. It also would ensure that companies outside the EU offering services to EU citizens or processing data of EU citizens must still comply with the Regulation.

See "*Cloud Data Protection*" Page 3

The Committee would like to recognize and extend a special thank you to out-going Co-Chair, **Rob Corbet**. We thank him for his leadership and dedication to the Committee over the past two years. Rob will now take over the role of the Committee's illustrious Immediate Past Chair.

Report on Russia's New Data Localization Law

By: Katie Woodcock

Everyone is talking about Russia's new data localization law and the possible impact on both multinational and non-Russian companies. The changes will require organizations to save personal information about Russian citizens within the territory of Russia. Although the actual interpretation of how the personal information needs to be saved within Russia is not entirely clear, many businesses are very anxious about the impact on their businesses and information systems. Furthermore, the pressure on impacted companies was recently increased by moving forward the enforcement date from September 2016 to January 1, 2015.

Additional details on Russia's Data Law are available at http://online.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920.

Chinese Bitcoin exchanges submits joint comments on the proposed "BitLicense" Proposal.

By Yankun Guo, The John Marshall Law School | J.D. Candidate 2015

As the deadline to comment on New York State Department of Financial Services (NYDFS)'s Proposed Regulation of the Conduct of Virtual Currency Businesses (BitLicense Proposal) approaches, the three main Chinese Bitcoin Exchanges submitted their comment on August 20, 2014. BTC China, Huobi, and OKCoin requested that:

> "(1) the BitLicense regime should cover only virtual currency businesses with meaningful connection to the State of New York; (2) a licensee's affiliates should have no obligation to allow the NYDFS to examine their respective facilities, books and records that are unrelated to the licensee's operations; and (3) The test for whether the performance of enhanced due diligence (EDD) on a customer is necessary should turn on whether the customer and the applicable licensee are from the same jurisdiction instead of whether or not the customer is a U.S. person."

The Chinese companies fear that the cross-border implications of the BitLicense Proposal could subject them to onerous regulations and diminish their capacity to operate and expand. The comment's first request goes to the broad definition of "virtual currency business activity," a result of which would be that if any Chinese, or foreign bit exchange for that matter, has even a single customer located in New York the exchange would be forced to comply with entire the BitLicense Proposal. The second request is to limit NYDFS's power to comprehensively examine the Exchange's business operations regardless of its relevance to virtual currency regulation. Finally, the third request to reconsider the burdensome EDD required for non-US persons addresses the absurdity of forcing foreign companies to conduct heightened diligence on what would be their local clientele as opposed to a New York client located half a world away. Still recognizing the need for a regulatory framework on virtual currencies, the Chinese companies hope to limit some of the cross-border implications of the current BitLicense Proposal.

[1] NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES PROPOSED NEW YORK CODES, RULES AND REGULATIONS (July 23, 2014), *available at*: http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf

[1] JOINT COMMENTS TO NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES ON THE PROPOSED REGULATION OF THE CONDUCT OF VIRTUAL CURRENCY BUSINESSES (Aug. 20, 2014), *available at:* https://com.btcchinacdn.com/docs/China%20Comments%20on%20Bitlicense.pdf

Cloud Data Protection… (Cont.)

In a survey conducted by security provider SkyHigh Networks of more than 7,000 cloud services, it is estimated that only 1% of current cloud providers would be compliant with the proposed EU Regulation, particularly the regulatory requirements pertaining to data residency, data breach detection and notification, encryption and data deletion policies. The proposed penalties for violation of these new laws can be up to 5% of a company's annual revenue or up to 100m Euro. This is in contrast to the Directive which did not provide guidance on applicable penalties. For companies doing business in or with the EU, this is significant in that considerable time and money will need to be spent to ensure compliance or risk incurring severe financial punishment.

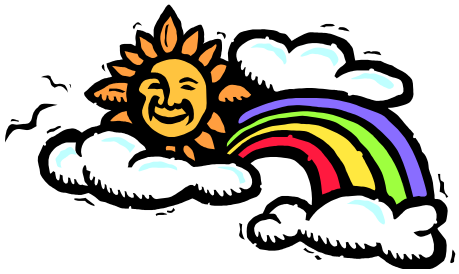
Data residency is of particular concern, as the Regulation requires that data not be stored or transferred through countries outside the European Economic Area that do not have equivalently strong data protection standards. Currently only 11 countries meet EU privacy requirements, and the U.S. is not among them, despite the fact that approximately 67% of all cloud services are headquartered in the U.S. The U.E.-E.U. Safe Harbor list provides a list of organizations that have notified the U.S. Department of Commerce that they adhere to the Safe Harbor Framework developed between the Department of Commerce and the European Commission to ensure compliance with EU laws on protection of personal data. However, only about 9% of U.S.-based providers have been awarded Safe Harbor Certification, which provides these companies with an exemption to the current EU Directive transfer restrictions. Currently, participation in the Safe Harbor Framework is voluntary and organizations self-certify their compliance. The U.S. Federal Trade Commission signed off on final orders this past June settling charges against 14 companies for falsely claiming Safe Harbor certification.

Despite the U.S.'s apparent moves forward in terms of compliance with EU data regulations, political stumbling blocks continue to emerge. Currently, legislation is planned that, once enacted by the U.S. Congress, will extend the protections of the U.S.Privacy Act, previously only available to U.S. citizens, to EU citizens as well. This would give EU citizens, among

Continued from page 1

other rights, the right to go to court in the U.S. to sue for improper use of their private data. U.S. Attorney General Eric Holder stated, "The Obama administration is committed to seeking legislation that would ensure that ... EU citizens would have the same right to seek judicial redress for intentional or willful disclosures of protected information and for refusal to grant access or to rectify any errors in that information, as would a US citizen." Nonetheless, the U.S. very recently instructed Europol, the EU's police agency, to withhold its own annual internal data protection review from disclosure to EU lawmakers due to the fact that the report was written without the consent and permission of the U.S. Treasury Department. The U.S. cited violation of security protocols and undermining of inter-agency trust and information exchange for its demand to withhold the report. EU Ombudsman Emily O'Reilly, in a letter to the European Parliament, rightly questioned whether it is acceptable that an agreement with a foreign government should prevent her from performing her duties.

Despite the conflict of national laws both within the EU and between the EU and the US and the bureaucratic inter-agency delays, it appears that strides are being made toward a consistent enforceable standard to which all companies dealing with data of EU citizens can be held. The economic implications of these standards on businesses dealing with private data of EU citizens may be significant in the short-term, but expenditures made to ensure compliance will be minimal in light of the penalty guidelines included in the proposed Regulation. The Regulation will unify the existing patchwork of data regulations among EU countries, and when coupled with the Safe Harbor Framework and the proposed legislation to extend U.S. Privacy Act protection and rights to EU citizens, a clear and definitive set of policies is taking shape to effectively handle the myriad issues arising from the global framework in which personal data exists.



Privacy – Brief Observations on the Evolution of Brazilian Legislation

By: Renato Blum

Attorney and economist; Renato, Vice-Chair of the Privacy, E-Commerce and Data Security Committee of American Bar Association Section of International Law. Recognized professional for 2 consecutive years in Chambers & Partners, Who's who and Best Lawyers; Invited speaker in several international conferences (EUROFORUM, LegalTech, SEDONA, ITECHLAW, HTCIA, ISSA, IAPP, Georgetown Law, etc.; Co-author of the article "Recent Development on Cyberspace Law: A View from Brazil" (THE BUSINESS LAWYER - American Bar Association – 2013), "Brazilian's Chapter" of Data Protection & Privacy Law (2nd Edition, European Lawyer - Thomson Reuters).Twitter: @opiceblum; www.opiceblum.com.br

It has frequently been noted in international circles that the relationship between Brazilians and the Internet represents a complex topic inside Brazil. The natural sociability of its people and their constantly growing use of social networking have resulted in legal practitioners being required to deal with an ever widening range of legal problems in relation to privacy.

It became apparent through the practice of applying the then existing legislation that these rules needed to be adapted in order that they could be more effective in preventing bad practices.

In the area of Criminal Law, although Decree 2848/1940 of the Brazilian Criminal Code already provided applicable legislation it was considered more satisfactory to have a specific law to punish those that violated the information privacy of others; this was satisfied through the entry into statute of law 12.737/2012

However prior to the introduction of this measure the legal system had resolved the need to deal with cases of the much feared disclosure of sensitive government information; Law 7170/1983 takes care of situations detrimental to national security.

Moving to consumer protection, Brazil has implemented a much praised Consumer Protection Code (Law. 8,078 / 1990), it requires that suppliers of goods and services (including those online) provide clear information to its customers, with systems to resolve issues in relation to damaged or defective goods. In 2013 Decree 7962 was passed, which brought into force regulations to simplify communications via the web, it being, for instance, obligatory to provide clear summaries of contracts and to offer effective customer service channels.

Finally, in 2014, after years of debate in the legislature, Law 12.965, The Internet Legal Framework or *Marco Civil da Internet* as it is known in Brazil was passed. The law defined amongst other things basic principles of privacy protection. Although it did also include some controversial provisions it is clear that the law reaffirms the right to freedom of expression and seeks to protect privacy on the basis that it is protected under the Brazilian Constitutional right to human dignity.

Introduction to Your New PEDS Leadership Team

W. Gregory Voss is an incoming Co-Chair of the Privacy, E-Commerce, and Data Security Committee. Last year he served as a Vice-Chair of the Committee and as a Co-Chair of the International Intellectual Property Committee (he is an Immediate Past Chair of that committee). He has been the PEDS Committee Year-in-Review editor since 2011.

Voss graduated from the University of Michigan Law School and obtained a post-graduate degree in Law and Information Systems from the Université Toulouse 1 Capitole in France. He is a member of the *Institut de Recherche en Droit Européen International et Comparé* (IRDEIC). Following work in private practice and as a company lawyer, Voss became a Professor of Business Law at the Toulouse Business School (TBS). He is admitted to practice law in New York and Toulouse and is a non-practicing solicitor in England and Wales.

Katie Woodcock is continuing another year as Co-Chair of the Privacy, E-Commerce, and Data Security Committee. She graduated from Golden Gate University School of Law and obtained a Master of Law in International and European Law at the University of Amsterdam. Following a brief stent as in-house counsel for an investment company, Katie joined the data protection and technology practices of Lorenz, a law firm in Brussels. She is admitted to practice law in California and listed on the B-list of the Brussels Bar.

Year-in-Review

Articles wanted…

The time has come to participate in drafting The Year-in-Review (YIR) edition for 2014. The YIR is prepared in cooperation with the SMU Dedman School of Law. Late each spring the Section of International Law publishes the YIR based on submissions from all the Section's committees. This is a great way to get some exposure for you and your organization.

We are therefore requesting you to consider submitting a short update of the most significant legal developments in your specialized area of privacy, e-commerce and data protection law for the year 2014.

If you are interested in submitting something, please respond to Committee Editor Gregory Voss (g.voss@tbs-education.fr) -- in order to express your interest no later than Wednesday, October 22, 2014. Submissions are due no later than November 14, 2014.

As part of your response, please provide a brief description of the topic you intend to cover (including geographic area), your name, e-mail address and telephone number.

Privacy, E-Commerce & Data Security Committee

Co-Chairs: Gregory Voss, Katherine Woodcock

Vice-Chairs: Brendan Berne, Tony Burke, Claudia Cantarella, Cecil Sae Hoon Chugn, Kyoung Yeon Kim, Micael Montinari, Kenneth N Rashbaum, Jose A Santos Jr,

Newsletter Editor: Adrianne Laneave

ABA Meetings and Other Happenings:

Check out our website!

http://apps.americanbar.org/dch/committee.cfm?com=IC736000

PEDS Mission Statement

The Privacy, E-Commerce and Data Security Committee has been established as a resource to assist in the education of international law practitioners on the evolving international laws and practices relating to privacy and data protection, in particular as they relate to global e-business, and to contribute to the development of policy and the promotion of the rule of law in those areas.

Committee Publications

W. Gregory Voss (2013) 'Privacy law implications of the use of drones for security and justice purposes', International Journal of Liability and Scientific Enquiry, Vol. 6, No. 4, pp. 171-192 (this came out in April 2014). A short introduction to this article was done by Prof. Ronald C. Griffin at Florida A & M University's College of Law and is available at http://www.inderscience.com/editorials/f397658142121011.pdf. In addition, the publisher Inderscience issued a press release on this article entitled "Watcher from the skies" and available at http://www.alphagalileo.org/ViewItem.aspx?ItemId=142078&CultureCode=en.

W. Gregory Voss (2014) 'Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later', Journal of Internet Law, Vol. 17, No. 9, March 2014, pp. 1 and 12-24.

W. Gregory Voss (20114) 'The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation', Journal of Internet Law, Vol. 18, No. 1, July 2014, pp. 3-7.

Upcoming Events...

2014 Fall Section Meeting

The **ABA SIL's Fall meeting in Buenos Aires** is just days away. The meeting is taking place at the Hilton from October 21 - 25, 2014. We encourage all members to attend and check out the PEDS sponsored panels:

- Privacy and Data Protection: Business and Social Media: Find more information here. Taking place Wednesday, 10/22: 11:00 AM - 12:30 PM
- The Right to be Forgotten in Latin America: Legislation, Cases in Law and Trend: Find more information here. Taking place Thursday, 10/23: 11:00 AM - 12:30 PM

2015 Spring Section Meeting

The **ABA SIL's 2015 Spring Meeting in Washington, DC** will provide cutting-edge programs with world-class speakers and materials on issues that will enhance attendees' professional skills including professional ethics. The programs will provide timely and practical guidance to attendees and should reflect the "best thinking" on private and public international law issues.

The International Law Section's 2015 Spring Meeting will take place from April 28 – May 2, 2015, at the Hyatt Regency on Capitol Hill in Washington. For program proposals or more information please email Katie Woodcock (katherinewoodcock@hotmail.com).