ISSN : 1875-4120
Issue : Vol. 14, issue 1
Published : January 2017

Transnational Dispute Management
www.transnational-dispute-management.com

Class Consciousness: Class Action Arbitration under U.S. and EU Privacy Laws by W. Sapronov and J. Srouji

About TDM

TDM (Transnational Dispute Management): Focusing on recent developments in the area of Investment arbitration and Dispute Management, regulation, treaties, judicial and arbitral cases, voluntary guidelines, tax and contracting.

Visit www.transnational-dispute-management.com
for full Terms & Conditions and subscription rates.

Open to all to read and to contribute

TDM has become the hub of a global professional and academic network. Therefore we invite all those with an interest in Investment arbitration and Dispute Management to contribute. We are looking mainly for short comments on recent developments of broad interest. We would like where possible for such comments to be backed-up by provision of in-depth notes and articles (which we will be published in our 'knowledge bank') and primary legal and regulatory materials.

If you would like to participate in this global network please contact us at info@transnational-dispute-management.com: we are ready to publish relevant and quality contributions with name, photo, and brief biographical description - but we will also accept anonymous ones where there is a good reason. We do not expect contributors to produce long academic articles (though we publish a select number of academic studies either as an advance version or an TDM-focused republication), but rather concise comments from the author's professional 'workshop'.

TDM is linked to **OGEMID**, the principal internet information & discussion forum in the area of oil, gas, energy, mining, infrastructure and investment disputes founded by Professor Thomas Wälde.

Presented at the Center for International Legal Studies (CILS) Symposium "**International Arbitration Symposium**" which was held in Salzburg, Austria, 2 - 5 June 2016. Chairs: Mr. Laurent Hirsch, Switzerland and Ms. Silvia Marchili, United States/Argentina. More information about CILS www.cils.org

Class Consciousness: Class Action Arbitration under U.S. and EU Privacy Laws[1]

by Walt Sapronov, Joseph Srouji[2]

Abstract

In recent years, regulators in both the U.S. and the European Union (EU) have been increasingly aggressive in privacy enforcement within their respective jurisdictions. The enforcement trend follows expanded privacy protections adopted by U.S. regulators (such as the Federal Communications Commission's recently announced "net neutrality" privacy rules, as well as the extra-territorial reach of EU data protection authorities following the invalidation of a trans-Atlantic accord that had governed cross-border privacy protections). This governmental enforcement trend creates a template for class action litigants seeking damages for those same privacy violations under private causes of action. In the U.S., well-established case law supports a defense to such class action exposure through the use of binding arbitration agreements with class-action disclaimers ("cut-off clauses"). This discussion examines this privacy litigation trend, the no-class action arbitration defense, and the implications for cross-border privacy disputes involving parties in the U.S. and the EU.

I. Introduction[3]

In recent years, regulators in both the U.S. and the EU have been increasingly aggressive in privacy enforcement within their respective jurisdictions. The enforcement trend follows expanded privacy protections adopted by U.S. regulators (such as the Federal Communications Commission's ("FCC") recently announced "net neutrality" privacy rules, as well as the extra-territorial reach of EU data protection authorities as part of the Data Protection Directive 95/46/EC. This reach has only increased in recent times, most notably with the invalidation of a trans-Atlantic accord (the so-called "EU Safe Harbor") that had governed cross-border privacy protections). This governmental enforcement trend creates a template for class action litigants seeking damages for those same privacy violations under private causes of action. In the U.S., well-established case law supports a defense to such class action exposure through the use of binding arbitration agreements with class-action

[1] The views expressed in this discussion are those of the authors and not those of any client or other party. This discussion summarizes the remarks made by Messrs. Sapronov and Srouji at the Center for International Legal Studies, International Arbitration Symposium, June 5, 2016; Session 15, Look into the Future–Opportunities and Challenges to Arbitration, http://www.cils.org/home/conference.php?ConferenceID=278&. For a more detailed discussion on the privacy laws discussed herein, See Sapronov & Associates, P.C. Client Alert: *Privacy Compliance and the New World Order* (April 13, 2016), available upon request at info@wstelecomlaw.com. While accurate to the best of our knowledge, this discussion is provided for tutorial purposes only and is not to be construed as a legal opinion or legal advice. Please contact us at +1 770-399-9100 or at info@wstelecomlaw.com if you have any specific questions about this topic or the disclaimer.

[2] Walt Sapronov is a Shareholder and Joseph Srouji (licensed in Paris, France only) is Of Counsel with the Firm of Sapronov & Associates, P.C. Angela Carter and Mathew Powers assisted in the preparation of this discussion. For more information on the Firm, visit www.wstelecomlaw.com.

[3] THIS DISCUSSION IS PROVIDED FOR TUTORIAL PURPOSES ONLY AND IS NOT TO BE DEEMED LEGAL ADVICE. PLEASE CONTACT US OR OTHER COUNSEL FOR LEGAL ADVICE REGARDING ANY OF THE ISSUES DISCUSSED HEREIN.

waivers (a "cut-off" defense). This discussion examines this privacy litigation trend, the arbitration cut-off defense, and their implications for cross-border privacy disputes involving parties in the U.S. and the EU.

Noteworthy here is that while U.S. class action jurisprudence is still rapidly unfolding, the trend appears to be one in favor of the defendants, whether through enforcement of the arbitration cut-off defense or, as established under a recent U.S. Supreme Court decision, *Spokeo, Inc. v. Robins*, through higher plaintiffs' burdens to show injury.

The second part of our discussion addresses the potential class action relief in EU jurisdictions, whether through judicial or arbitration remedies. The issue discussed here is whether privacy and data breach violations involving cross-border transfers are actionable on class-wide basis in EU jurisdictions.

Historically, the answer would be no. But while Europe does not have a US-style litigation culture, there are nevertheless some initial signs that the EU may be moving in that general direction.

II. U.S. Privacy Enforcement and Recent Class Action Litigation

A. Privacy Compliance in the U.S.

To repeat, privacy compliance in the U.S. has always been challenging as domestic privacy laws are a patchwork of federal and state statutes and regulations (some varying by industry), common law principles and :best practices."[4] Over the last few years, under increasingly aggressive privacy enforcement by federal and state regulators, the penalties for non-compliance have increased. So have the chances of being named as a defendant, as many U.S. privacy laws are actionable under multiple, overlapping jurisdictions.

Thus, the FCC,[5] the Federal Trade Commission ("FTC")[6] and various state attorney generals have expanded their administrative authority with multi-agency enforcement actions for the same offense. The recent Dish litigation illustrates such "piling on" by federal and state agencies for privacy violations,[7] and a recent "Memorandum of Understanding" between the FCC and FTC gives public notice of the agencies' intention to "work together" in such coordinated actions where the agencies exercise concurrent jurisdiction.[8] The trend is coupled with expansive interpretation of statutory privacy protections under the Communications Act,

[4] A discussion of these myriad U.S. privacy laws is beyond the scope of this alert. For a general overview, see W. Sapronov, *"Drafting Privacy Clauses in Technology Contracts,"* Presentation Materials for Georgia State Bar, Technology Law Institute (October 29, 2013).

[5] See 47 U.S.C. §222 (obligating carriers to protect subscribers customer proprietary information (CPNI)); 47 USC Chapter 5, Subchapter VI (Penal Provisions; Forfeitures) §§501-510.

[6] Federal Trade Commission Act (15 U.S.C. §§41-58). See *e.g.*, Wyndham Worldwide Corp., 799 F.3rd 236 (3rd Cir. N.J. 2015).

[7] See https://www.ftc.gov/news-events/press-releases/2015/01/court-grants-partial-summary-judgment-ftc-case-against-dish *U.S. et al. v. Dish Network LLC*, case number 3:09-cv-03073, (D. Ill. 2014), (granting partial summary in federal prosecution of "robo-calling" by Department of Justice on behalf of the FTC, brought concurrently with four state plaintiffs).

[8] See https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

the Federal Trade Commission Act, the Telephone Consumer Protection Act[9] and numerous state privacy laws by the respective agencies charged with their enforcement.

From the defendants' standpoint (for alleged privacy violations), all of this will likely get much worse.

On June 13, 2016, the U.S. Circuit Court of Appeals for the District of Columbia released its long-awaited decision on the FCC's most recent adoption of Open Internet (a/k/a "net neutrality") rules, affirming them by a 2-1 vote.[10] While an appeal for review to the U.S. Supreme Court is likely, the decision supports the FCC's proposed adoption of expanded privacy protections to include subscriber information delivered under both "traditional" telephone and under modern broadband Internet connections. In recent years, the FCC had already stepped up its privacy enforcement.[11] Now, supported by the affirmation of the Open Internet Order, the agency's newly proposed, expansive privacy protections will both broaden the categories of protected information delivered over broadband connections and expand the agency's carrier privacy (so-called "CPNI") regulations (applicable to "traditional" telecommunications carriers) to broadband internet access providers – a much larger pool of defendants.[12]

Further, the FCC and FTC have formally announced cooperation in privacy enforcement,[13] even as the FTC has expanded its privacy enforcement actions to include companies' liability for failure to protect consumer data from cyber-attacks.[14] So too have state authorities under their respective state data breach notification and other state privacy laws.[15]

Finally, many U.S. privacy laws support a private cause of action,[16] thus adding to the possibility that civil claims - including class actions - will follow the governmental ones.

---

[9] 47 U.S.C. §227; 16 C.F.R. §310; and 15 USC §6101, *et seq*.

[10] *Protecting and Promoting the Open Internet*, 80 FR 19737 (2015), aff'd sub. Nom. *U.S. Telecom, et. al. v. FCC*, No. 15-1063, slip op. (D.D.C. June 14, 2016). See also https://federalregister.gov/a/2015-07841.

[11] See, *e.g.*, *In Re AT&T Mobility, LLC, Notice of Apparent Liability for Forfeiture and Order*, FCC 15-63 (June 17, 2015) (assessing unprecedented $100 million dollar fine against AT&T for offering "unlimited data plans" without adequately disclosing specific access speed restrictions and other limitations, a violation of FCC Open Internet rules).

[12] See 47 U.S.C. § 222 (obligating telecommunications carriers to protect customer proprietary network information and to exercise other privacy protections); 47 CFR Part 64 (Subpart U) §§ 64.2001-64.2011 (codifying customer proprietary network information (CPNI) and other carrier privacy rules). *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 81 FR 23359 (April 20, 2016) (proposing to extend privacy regulations to Broadband Internet Access Service (BIAS) providers).

[13] https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

[14] *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236, 245 (2015) (holding that where a company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business, this meets the definition of unfair practice under the FTC unfair trade practices rules).

[15] See, *e.g.*, People v. Delta Air Lines, Inc., Cal. Super. Ct., No. CGC 12-526741, (dismissed sub. Nom. May 9, 2013).

[16] See, *e.g.*, 47 USC §§ 207-208 (creating private cause of action and prescribing remedies for recovering damages for any person for claiming to be damaged by any common carrier).

B. Nemesis Follows Hubris: Private Actions Often Follow Regulatory Enforcement

For those corporate defendants unfortunate enough to have been targets of governmental privacy enforcement, their exposure to privacy actions – typically brought as class actions – is all but inevitable. The governmental enforcement action, as it is now customarily concluded with an admission of liability (not just a consent decree), creates a template for private class actions, as the record creates admissions and other evidentiary support.

The pattern may be seen in recent, much publicized data breaches involving companies such as AT&T, Sony, Home Depot, Target, and others.[17] Examples of such claims typically include negligence claims for failure to maintain adequate security measures giving risk to foreseeable risk of harm.[18] Such claims can also be brought as derivative shareholder actions, especially where the defendant is a public company subject to the Securities & Exchange Commission's ("SEC") reporting rules. The SEC has recently issued guidance requiring such companies to disclose data breaches that may have a material impact.[19]

C. Mandatory Arbitration and Class Action Cut-off Defenses

But there is some good news for defendants. In recent years, putative class action plaintiffs have faced a defendant-friendly judicial trend supporting (with some exceptions) both the enforcement of class-action cut-off defenses in consumer contracts and, more recently, raising the bar for plaintiffs' requirements for the showing of damages in such cases.

Typically, class action waivers include mandatory arbitration clauses that consumers must agree to (often by "click wrap" to an online terms and conditions) as a condition of purchase. For example, such mandatory online agreements are customarily found in telecoms or Internet access agreements, where the terms and conditions are posted online. While some states will permit challenges to the enforceability of such agreements under consumer protection or unconscionability defenses, the U.S. Supreme Court, commencing with its seminal decision, *AT&T Mobility v. Concepcion*, has broadly validated such arbitration clauses with class action cut-offs, holding that the Federal Arbitration Act (FAA)[20] preempts state consumer protection laws that disallow class action arbitration.[21] Another recent Supreme Court decision, *American Express v. Italian Colors*, applied the *Conception* holding to uphold a waiver of class arbitration of federal antitrust claims.[22] So did another U.S. Supreme Court decision, *DIRECTV v. Imburgia*, following the *Conception* reasoning to enforce a similar class-action waiver in an arbitration agreement, finding the lower courts' interpretation of the waiver inconsistent with the Supreme Court's rulings on arbitration and class-action waivers.[23]

---

[17] See generally, J. C. Herman, "Data Breach Liability on the Rise", presented at Law Seminars International, TECHNOLOGY AND CLOUD TRANSACTIONS, Conference, Atlanta, Georgia, April 27-28, 2015

[18] *Id*. (citing, *e.g.*, In Re Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522 (PAM/JJK) (USDC Minn.), Dkt. No. 261, December 2, 2014)(denying motion to dismiss class action claims and specifically rejecting argument that defendant Target corporation not liable for risk of third party criminal acts).

[19] Securities and Exchange Commission / CF Disclosure Guidance: Topic No. 2 / Cybersecurity / October 13, 2011.

[20] 9 U.S.C. § 1, *et seq.*

[21] *AT&T Mobility v. Concepcion*, 563 U.S. 321 (2011) (holding that the Federal Arbitration Act preempts state laws that disallow class action arbitration waivers).

[22] *American Express Co. v. Italian Colors Restaurant*, 133 S.Ct. 2304 (2013).

[23] *DIRECTV, Inc. v. Imburgia*, No. 14-462, 577 U.S. [___], 136 S.Ct. 463 (2015).

As further illustration of this class-action cut-off defense, in a recent case involving Cox Communications, Inc. ("Cox"), four class action plaintiffs sued for false advertising and for recovery of improper fees charged by Cox, ignoring the arbitration and class action cut-off clause in Cox's customer agreements. Cox removed the case to Federal Court,[24] which granted Cox' motion to compel arbitration or, in the alternative, to dismiss for failure to state a claim.

In its Motion, Cox contended that each of the plaintiffs agreed to a binding and broad mandatory arbitration clause that included a class-action cut-off among other waivers.[25] Citing *Concepcion* for the "liberal federal policy favoring arbitration agreement", the Court rejected Plaintiffs' arguments that the arbitration clauses were unenforceable for reasons such as lack of notice and consent, and unconscionability. Even under consumer-friendly California law, the Court found that an arbitration clause within a contract may be binding on a party even if the party never actually read the clause, that the arbitration clause in question (with its opt-out provisions) was prominent and conspicuous, and that the plaintiffs had sufficient notice and consented to the arbitration clause.[26]

D. Still More Defendant-Friendly U.S. Supreme Court Precedent

There is still more defendant-friendly U.S. precedent.

On May 16, 2016, the U.S. Supreme Court issued an opinion in *Spokeo, Inc. v. Robins*[27]. In *Spokeo*, plaintiff alleged that Spokeo published inaccurate information about his background and employment status in its online database, and that an unspecified individual accessed that information. The plaintiff claimed that this disclosure caused lost employment opportunities and filed a class-action lawsuit for a violation of the Fair Credit Reporting Act of 1970, 15 U.S.C.§1681 *et seq.*.

The District Court dismissed the plaintiff's complaint for lack of standing, but the Ninth Circuit Court of Appeal reversed, finding that the plaintiff had adequately alleged injury in fact, a requirement for standing under Article III of the U.S. Constitution. The U.S. Supreme Court remanded, finding that the Ninth Circuit focused only on the "particular" harm suffered by the plaintiff, and not the additional requirement that such harm be "concrete" as required for standing. The Court noted that "intangible injuries can nevertheless be concrete," but held that the appellate court had failed to address whether "the particular procedural violations" alleged by the plaintiff "entail a degree of risk sufficient to meet the concreteness requirement." *Spokeo* at 11.

Although the Court did not address the merits of the plaintiffs' claim in *Spokeo*, the decision strongly suggests that allegations of "harm" for standing purposes will be strictly construed in the context of a breach (or other allegedly improper disclosure) of private information contained in an online database. This precedent could arguably apply to other contexts where harm from data breaches may be difficult to identify or establish. This could conceivably

---

[24] *Matti Yousif, et al. v. CoxCom, LLC, et al.* (Case No. 3:15-cv-01499-JLS-MDD) (S.D. Cal. 2015).
[25] Cox Motion, pp. 6-10.
[26] Cox Order, 5:21-26; 12:1-13:20; 15:18-16:14. *But see Griswold v. Coventry First LLC, et al.*, 2014 U.S. App. LEXIS 15362 (3rd Cir. Aug. 11, 2014) ("*Griswold*") (holding that a non-signatory party to a purchase agreement was not bound by the agreement's arbitration clause). An analysis of the contract formation issues distinguishing *Griswold* from the Concepcion line of cases is beyond the scope of this discussion.
[27] *Spokeo, Inc. v. Robins*, No. 13-1339 (U.S. May 16, 2016) ("Spokeo").

apply to both private litigation and government actions (such as by the FCC and the FTC) against corporate defendants that fail to protect online personal information, for example, as a result of a cyber-security breach.

III. The Trend "Across the Pond"

A. EU Privacy Enforcement and Class Actions - New Exposures

Recent developments continue to shed light on the rapidly changing privacy landscape evolving in Europe, which have a significant impact on international data transfers as well as the risks for companies engaging in such transfers. In the case *Maximillian Schrems v Data Protection Commissioner*[28] the Court of Justice of the European Union (CJEU) took a bold step forward, invalidating a 15-year-old agreement between the EU and US while granting increased powers to EU Data Protection Authorities (DPAs). Since it's inception, Safe Harbor was widely viewed by privacy professionals as a band-aid of sorts: a necessary compromise to accommodate the greater goal of international commerce.

Nevertheless, its invalidation came as a surprise to even the most veteran privacy specialists, as well as sent a shock-wave across international firms' legal departments. While offering a brief transition period for companies to get their house in order, DPAs were nevertheless explicit in their desire to enforce the court's decision. And such enforcement came in June when the Hamburg Data Protection Commissioner levied modest fines against Adobe Systems, the fruit juice maker Punica (subsidiary of PepsiCo) and Unilever (totaling some 28,000 euros) for continuing to rely on the defunct Safe Harbor agreement. The German DPA made clear that stricter fines for other non-compliant companies would be coming.

Given saber-rattling from regulators, EU and US officials were under considerable pressure to devise a bigger band-aid. The "Privacy Shield" was officially adopted by Adequacy Decision of the EU Commission on 12 July and will allow US companies to formally adhere to the protocol beginning August.[29] The path to adoption was a bumpy one, however, and doubts linger as to how effective Privacy Shield will be in resisting legal challenges, most likely to come from the CJEU.

The Article 29 Working Party (WP29), led by its chairwoman Mrs. Falque-Pierrotin, was particularly critical prior to its formal adoption in regards to the inherent weaknesses in the agreement. And to make matters worse for supporters of the Privacy Shield, Giovanni Buttarelli, European Data Protection Supervisor (essentially the watchdog for EU institutions' privacy compliance with a broader advisory role), took further aim at the agreement prior to approval calling it "not robust enough" as part of a white paper issued in May.[30] Such opposition provides ready fodder to DPAs (notably those in Germany) to use their reinforced post Safe-Harbor powers and also creates uncertainty if the agreement will survive its one-year renewal in 2017.

---

[28] (CJEU C-362/14).

[29] C(2016) 4176 Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

[30] Opinion 4/2016: Opinion on the EU-US Privacy Shield Draft Adequacy Decision, European Data Protection Supervisor, 30 May 2016; also the European Parliament also issued a resolution in May (2016/2727 (RSP)) calling for the Privacy Shield agreement to be renegotiated.

In the wake of these political and transatlantic developments, the adoption of the General Data Protection Directive (GDPR) – some two years in the making – almost went unnoticed. The GDPR is by far the bigger story since it replaces Data Protection Directive 95/46/EC, essentially providing a complete legal overhaul while retaining essential time-tested provisions. It also signals a new era of both harmonization in EU privacy law (with the exception of specific areas like health data, where EU member states can adopt stricter standards) as well as enforceability given the strict sanctions regime (fines of up to 4% of global turnover or 20 million euros possible for certain offenses).

Recent fines by DPAs continue to be modest, with companies like Google and Facebook being favorite targets of the regulators. More troublesome for large international companies is the bad press, which can take a toll on their image and potentially erode their customer base. DPAs are indeed pleased that the GDPR will give them a bigger bite. And in the case of France, the ability of the CNIL to issue GDPR-like sanctions may come well in advance of the GDPR's official two-year transition period thanks to the recent "For a Digital Republic" bill, which aims, among other things, to modify Article 47 (administrative sanctions) of the French Data Protection Act.

Companies are thus faced with a new and complex legal and compliance landscape that will require greater risk analysis to ensure that privacy practices are compliant with the GDPR. This equates to revisiting information technology protocols on security, staffing up legal and compliance departments with qualified Data Protection Officers (soon to be required under the GDPR in some circumstances), adopting processes like Privacy by Design and Privacy Impact Assessments. The list is a long one but the guiding principle should be that regulators expect companies – either as data controllers or processors – to be held fully accountable for their privacy practices. Accountability is the new norm.

B. Privacy Torts and Class Actions – On the horizon?

This changing judicial and legislative landscape in the EU is compounded by other recent case law developments, which are slowly making privacy violations easier to qualify as genuine torts (even in the absence of pecuniary damage). In addition, privacy violations are also inching into the realm of class actions. While there is still a long way to go – and in no way is Europe near the threshold of a US-style litigation culture – there are nevertheless some initial signs that the EU may be moving in that general direction.

First, as a starting point it should be noted that EU courts have been reluctant to award damages for privacy violations – as it is often difficult to prove a monetary harm – and that class actions are all but of unheard of. However, the 2015 case of *Google v. Vidal-Hall* decided by the English Court of Appeal[31] may prove a significant turning point. It deviated from previous decisions, most notably that of *Johnson v MDU*,[32] by broadening the scope of privacy damages beyond having to prove uniquely pecuniary loss (Section 13(2) of the Data Protection Act of 1998). The court held, "[s]ince what the [Data Protection] Directive purports to protect is privacy rather than economic rights, it would be strange if the Directive could not compensate those individuals whose data privacy had been invaded by a data controller so as to cause them emotional distress (but not pecuniary damage)."

[31] *Google v Vidal-Hall* [2015] EWCA Civ 311 - A2/2014/0403.
[32] EWCA Civ 262; (2007) 96 BMLR 99.

Secondly, class actions are starting to enter the vocabulary of EU legal professionals and the public alike. Class actions were formally introduced into French law, for example, in 2014 (law "Hamon" of 17 March 2014 – now part of the French Consumer Code – and later modified to include the health sector and discrimination) with the specificity of allowing consumers to launch collective action provided, among other things, the action is spearheaded by a government approved consumer-interest group (*association*) and involves a consumer- or competition-related material prejudice. In practice such class actions have been slow to gain traction with roughly a half-dozen filed to date. And class actions for privacy breaches are not (yet) on the radar (at least not in France).

Mr. Schrems seems determined to continue setting trends, having launched a class action against Facebook in 2014, filed in an Austrian court against the firm's European HQ subsidiary based in Ireland. The case regrouped some 40 thousand users of the social network seeking a modest sum each in damages for Facebook's failure to comply with EU data protection laws, including the illegal tracking of their data as part of the US mass surveillance program. While Austria is reputed as class-action friendly, the case was struck down as a class action, leaving uncertainty as to how and when class actions for privacy violations will enter the vocabulary of EU legal specialists. Given the GDPR and political turbulence caused by Safe Harbor and Privacy Shield, the more pressing issue appears to be the risk of sanctions for privacy violations – especially cross-border data transfers – imposed by EU privacy regulators.