© 2016 ARMA International

## Data Privacy Meets a World of Risk:

# A Landscape in Turmoil

**John C. Montaña, J.D., FAI**

© 2016 ARMA International

2016 continued a tumultuous string of years for privacy law and for those charged with implementing it and managing the records affected by it. Prior years saw an assortment of inter-governmental squabbles related to eavesdropping by U.S. intelligence agencies, disputes over intelligence sharing for counter-intelligence purposes, and ongoing concerns in Europe over the adequacy of the Safe Harbor arrangement between the European Union (EU) and the United States.

In each of these cases, there was tension between the purported need to make information transfers and the countervailing desire of governments or individuals to keep information private. The cases created issues for organizations outside of government, caught as they often were between conflicting demands and responsibilities on both sides of the Atlantic and their own needs to use personal information for business purposes.

## Safe Harbor Gives Way to Privacy Shield

These issues were distilled in *Schrems v. Data Privacy Commissioner* (C-362/14 (Oct. 6, 2015)), in which law student Max Schrems sued in the European courts, alleging that Facebook's policies and practices violated EU data privacy law, and, thereby, so did the Safe Harbor Agreement, which permitted transfer of EU data from the EU to the United States under specified conditions.

### *Shield Cedes Power to DPAs*

Late in 2015, after years of litigation, the European High Court of Justice in the *Schrems* case finally issued a ruling. The decision did not, strictly speaking, invalidate the Safe Harbor Agreement. Rather, the court ruled the agreement was nonbinding on national data privacy authorities (DPAs), throwing 20 years of practice and doctrine into a state of great uncertainty.

The *Schrems* decision had the effect of allowing a national DPA to find a violation for *any* data transfer to the United States. Given the extent and duration of data transfer that had occurred, and the scope of potential penalties – up to 4% of a company's worldwide revenue – this new DPA power was, and remains, a matter of considerable concern to all.

## Data Privacy Regulation Brings Little Relief

2016 at first seemed to have brought relief from the court's decision. Early in the year, the European Union published the new General Data Privacy Regulation (GDPR), as well as the EU-U.S. Privacy Shield Agreement, which were intended to relieve the uncertainties arising from the Safe Harbor Agreement – and its demise in the courts – and from the ongoing problems organizations faced with the pre-existing privacy regime and its 28 country-specific privacy regimes.

### *Litigation Threatens Privacy Shield*

The small relief from these developments may be short-lived, however. The successful plaintiff in the Safe Harbor litigation has already made it clear that he's dissatisfied with the terms of the Privacy Shield and intends to litigate it. Thus, even before it had been formally adopted by the parties, Privacy Shield faced an uncertain future that is not likely to be decided for several years.

Parties who relied on Safe Harbor, and who then looked to Privacy Shield to permit cross-border data to continue, are now faced with an extended period of uncertainty as Privacy Shield slowly works its way through the courts. Given the scope of those transfers, the underlying value of the business they represent, and the near impossibility of unwinding already-comingled data sets should Privacy Shield ultimately be invalidated, this is very high-value uncertainty indeed.

### *GDPR Fails to Unify Rules*

The GDPR likewise offers far less certainty than it seems to at first glance. In theory, it replaces as many as 28 sets of rules that an organization might be subject to with a single set of rules. Except that it does no such thing.

Under the prior regime, national DPAs had complete autonomy – they answered to no one, and all promulgated such rules as they saw fit, applicable to organizations operating within their jurisdiction. This has not changed; each still has plenary and unchallengeable authority. And therein lies the rub.

Although the GDPR encourages DPAs to cooperate and to develop a single set of rules for any organization, they are not actually required to. So, maybe this will happen and maybe it will not. There is no mechanism to

Despite this year's passage of the EU-U.S. Privacy Shield agreement and the EU's General Data Privacy Regulation, the privacy landscape remains unstable, leaving organizations uncertain about their next steps. This article explores the causes of the instability and suggests how organizations might respond.

© 2016 ARMA International

force such things, and, in fact, the GDPR reaffirms each DPA's absolute independence and authority. As a result, organizations must now play this hand and discover how it's really going to work – which will again take several years to shake itself out, even under the best of circumstances.

ing some things. Maybe they will, but maybe they will not. So, again, organizations are forced into a waiting game to see if what amounts to wishful thinking by the EU authorities actually results in changes on the ground that will make the issues simpler.

long look at whether the concept of data privacy has perhaps swung too far in one direction. This could play itself out in a couple ways.

### *Legislation May Loosen Restrictions*

First, there might be legislative changes that relieve restrictions on such things as data transfer, short mandatory periods of retention, or data sharing. As the *WSJ* articles point out, such relief would significantly improve the capabilities of law enforcement, which has found itself hampered by aggressive, privacy-driven retention policies, or by the fact that existing data is subject to transfer and sharing restrictions. This is, in fact, what France and Germany, and no doubt other countries, are contemplating.

That, however, is a relatively long-term solution, if ever it comes, and it would result in changes only to those matters directly specified by the legislation.

Quicker and broader relief might come much sooner in the simple form of lax interpretation and enforcement.

### *Enforcement May Be Weak*

This would be nothing new. Safe Harbor – and privacy compliance generally – have always been to some extent a sham. Organizations claimed compliance with a complex set of laws they barely understood and frequently violated; as long as the organizations stayed under the radar and did nothing egregious, the European authorities turned a blind eye towards what was happening. Enforcement has generally been directed at high-profile offenders with deep pockets, such as Facebook and Google.

At the end of the day, the GDPR's harmonized rulemaking process amounts to little more than a series of suggestions to the national DPAs that maybe they should consider changing some things.

Even if it plays out as planned, there may well be very disparate results. The EU countries have taken different approaches to privacy, ranging from extremely prescriptive and detailed regulation in places such as France and Germany, to a relatively light hand in places like the United Kingdom – whose impending exit from the EU (i.e., "Brexit") ensures additional complication.

That means an organization based in France, whose DPA is supposed to manage the rules-rationalization process for it, could well find itself subject to a much more prescriptive and challenging set of rules than one fortunate enough to be based in, say, Ireland.

The GDPR likewise does not affect the current rules quagmire. Rules currently in effect remain in effect, and national DPAs are in no way inhibited from enacting new rules in line with their existing philosophies. The most that can be done is to delay a rule's implementation for a year if the authorities at the EU level disagree with it. And, again, those rules vary widely from country to country and are likely to continue to vary.

### *Organizations Must 'Wait and See'*

At the end of the day, the GDPR's harmonized rulemaking process amounts to little more than a series of suggestions to the national DPAs that maybe they should consider chang-

All of this poses significant questions to trans-Atlantic organizations and to those operating only within the EU: "Should we gamble on the continuing viability of Data Shield, or should we plan a future with more restrictive transfers of data outside the European Union? Can we plan on a single rule set within Europe, or must we continue to deal with multiple regimes? And what about Brexit?"

Making a significant change in management practice based on an assumed future is likely to be expensive: vast data sets might somehow have to be parsed out; new systems designed, built, and configured; and long-standing business practices changed. It could all be bad enough if the guess is right, but possibly catastrophic if the guess is wrong.

## Terrorism May Force Direction Change

An entirely countervailing influence arises from the issue of terrorism. Europe has been shaken in 2016 by deadly terrorist acts. And, as authorities investigate the incidents and seek to prevent future ones, they find themselves hampered by the restrictiveness of their own privacy laws. Two of the countries with the most restrictive laws, France and Germany, have been hit particularly hard by terrorism. According to two recent *Wall Street Journal* (*WSJ*) articles, both countries are taking a

© 2016 ARMA International

Schrems and the lawsuit that ultimately brought down Safe Harbor put a spotlight on data management practices, but terrorism concerns could change it right back. DPAs, legislators, and judges in the EU face the question of how tightly they want to enforce whatever privacy law may be in effect, and the reality that zealous privacy enforcement may well – and sometimes clearly does – conflict with effective law enforcement and counterterrorism activities.

Given that reality, Schrems may well find a less receptive audience for his future arguments. The more terrorist attacks there are in Europe, the more likely this is to be true. And, ultimately, data privacy is what the DPAs and the courts say it is. If they choose to see it – and enforce it – less restrictively, legal theories to the contrary will not count.

## In the Meantime…

So where does all of this leave organizations? That's a question whose answer has multiple parts.

### *Use the Privacy Shield*

First, because Privacy Shield is for now the law of the land, organizations should avail themselves of its protections. It would take years to get a lawsuit through the courts, and in the meantime a lot can happen. Further, there's no guarantee the next ruling will be a winner. At worst, Privacy Shield buys an organization a few years; at best, it's all that's needed.

### *Lobby for Rules Unification*

Organizations can ask the DPA in their jurisdiction to work with the other DPAs to develop a single regulatory framework. Their worst result would be a unified regime that's as bad as the worst one they're subject to now, which means there's little downside to such a move. More likely, nothing substantive would come of it. But there's always a chance that things could actually get better.

### *Build in Privacy Controls*

If building or configuring new systems, build them to minimize data privacy problems in the first place. Much of the need for Safe Harbor and Privacy Shield arises from the fact that people built systems and moved data first and thought about data privacy laws second.

### *Wait for More Change*

Beyond that, wait. It will take much time before the national DPAs, courts, and other relevant parties figure out how to operate in the new landscape. Until they give a clear indication of where they're going, it's much too early to reconfigure existing systems or rearrange complex business processes, with all the attendant costs and issues. To repeat, a wrong guess now could indeed be costly later.

On the other hand, it's not a good idea to assume nothing will ever change. Very likely, there will be substantive changes to the landscape that will require changes for organizations. Indeed, the best path is to wait and watch, while keeping all options open as long as possible. **END**

*John C. Montaña, J.D., FAI, can be contacted at* jcmontana@montana-associates.com. *See his bio on page 47.*