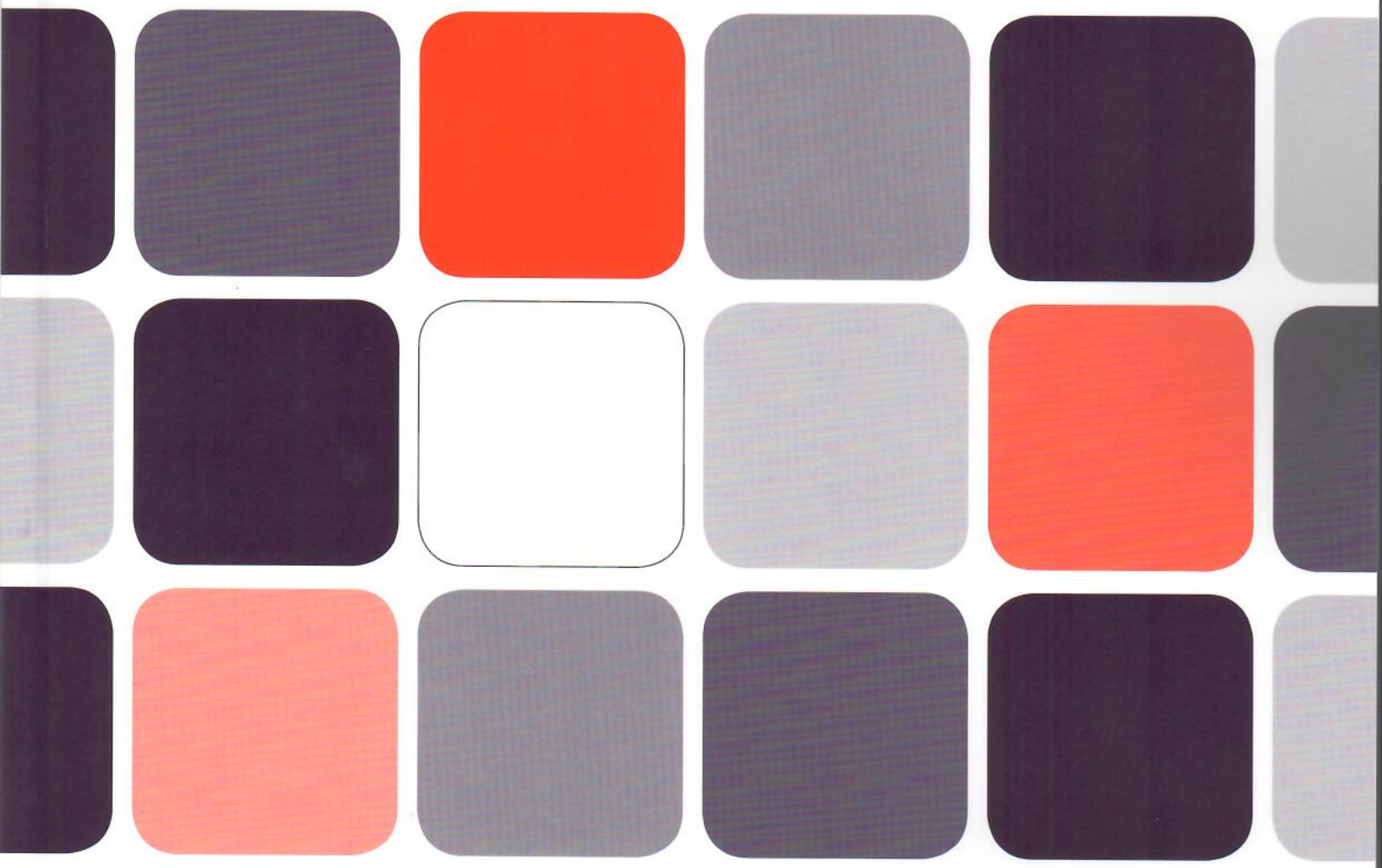
VOLUME ONE
NUMBER THREE
SUMMER 2017

ISSN: 2398-1679

Journal of

Data Protection & Privacy



GO DPO® | EU Compliance Ltd

Available online

HENRY STEWART PUBLICATIONS

Journal of
Data Protection & Privacy
Volume 1 Number 3

Contents

Henry Stewart Publications
Russell House
28/30 Little Russell Street
London WC1A 2HN, UK
www.henrystewartpublications.com

Henry Stewart Publications
North American Subscriptions Office
PO Box 361
Birmingham
AL 35201-0361, USA

Class action and data privacy in the USA and Europe: Effective deterrent or ill-founded approach to compliance?

Received: 12th June, 2017

Joseph Srouji
is a member of the Paris bar and founding partner of Srouji Avocats. His previous roles include Senior Counsel for Data Protection & Regulatory Affairs at GE Capital, where he specialised in data protection, financial and banking regulation and compliance, and Data Protection Officer for the French Data Protection Authority (CNIL), where he managed data protection for both the GE corporate group and capital businesses in Europe. He also teaches graduate law classes at Université Paris II Panthéon — Assas, where he completed his law degrees.

Srouji Avocats, 11 Blvd Sébastopol, Paris 75001, France
Tel: +33 (0) 1 78 64 64 83; E-mail: joseph.srouji@sroujiavocats.com

Margaux Dolhem
is completing her legal internship at Srouji Avocats as she finishes her law degree prior to taking the French bar exam. She worked as a legal assistant at Tramater SA in 2016 and interned at Galerie Kamel Mennour in the summer of 2015. She is completing her Master 2 in IP/IT law (Droit du multimedia et de l'informatique) at the University Paris 2 Panthéon — Assas and has an MA in business law and the history of art at University Paris 1 Panthéon — Sorbonne and a BA in law and the history of art.

Srouji Avocats, 11 Blvd Sébastopol, Paris 75001, France
Tel: +33 (0) 1 78 64 64 83; E-mail: margaux.dolhem@sroujiavocats.com

Abstract The class action lawsuit: a term that strikes fear into boardrooms and among executive circles in the USA, and one that provokes strong reaction in Europe, mostly as a metaphor for a litigation culture run awry. Despite the bad press, however, the class action has its backers and European policy makers have increasingly come to accept its merits, notably its potential as a way to extend the arm of government-sanctioned authority and more generally to edge companies towards compliance. This paper focuses on class actions generally and specifically on data privacy class actions, which are but one litigation channel for a plaintiff to pursue when it comes to privacy violations (notwithstanding current trends for cyber security-related shareholder derivative suits). It begins by recapping the fundamentals of class actions in the USA, the historical roots, procedural aspects and current trends; it then turns to Europe, in particular to France. France offers a unique glimpse into how Europe, more generally, is attempting to leverage the benefits of class actions while avoiding the perceived negatives, most importantly by keeping lawyers at distance when it comes to initiating class actions. The paper will then cover a few other EU jurisdictions for comparison purposes and provide an overview of the most well-known privacy class action to-date — that introduced by Max Schrems.

KEYWORDS: privacy, data protection, class action, Europe, France, litigation

INTRODUCTION

The class action lawsuit: a term that strikes fear into boardrooms and among executive circles in the USA, and one that provokes strong reaction in Europe, mostly as a metaphor for a litigation culture run awry. Despite the bad press, however, the class action has its backers and European policy makers have increasingly come to accept its merits, notably its potential as a way to extend the arm of government sanctioned authority and more generally to edge companies towards compliance.

While US class actions have historically been known for addressing ills in consumer fraud, labour and employment, securities and products liability — to name the most well-known — data privacy litigation is rapidly gaining ground as litigators step in to complement the reach of the US authority in the matter, the Federal Trade Commission (FTC), making headlines by launching aggressive class actions against major retail names such as Target and Wal-mart, or against the manufacturers of such mundane things as We-vibe 'toys'. With millions in settlement dollars there for the taking, nothing is off limits.

This paper focuses on class actions generally and specifically on data privacy class actions, which are but one litigation channel for a plaintiff to pursue when it comes to privacy violations (notwithstanding current trends for cyber security-related shareholder derivative suits). It begins by recapping the fundamentals of class actions in the USA, the historical roots, procedural aspects and current trends; it then turns to Europe, in particular to France. France offers a unique glimpse into how Europe, more generally, is attempting to leverage the benefits of class actions while avoiding the perceived negatives, most importantly by keeping lawyers at distance when it comes to initiating class actions. The paper will then cover a few other EU jurisdictions for comparison purposes and provide an overview of the most well-known class action to-date, introduced by none other than Max Schrems of Safe Harbor fame.

CLASS ACTIONS IN THE USA: A MODEL FOR INSPIRATION, OR ONE TO BE AVOIDED?

While the goal of this paper is not to cover the substantive procedural details of US class actions, some basic principles need to be addressed, including some historical context, to facilitate the comparative analysis. The class action procedure in the USA, encapsulated at the federal level and emulated in some shape or form in most state laws, is enshrined in Rule 23 of the Federal Rules of Civil Procedure. Under Rule 23(a), there are four prerequisites to any class action, commonly referred to as the principles of *numerosity*, *commonality*, *typicality* and *adequacy of representation*.[1]

First, the class must be 'so numerous that joinder of all members is impracticable'. While some class actions have been certified with as few as 35 members, usually class actions involve hundreds, thousands or in some cases millions of members to the class. Second, there must be questions of law or fact common to the class'. Third, the lead plaintiff may sue if their claims are 'typical of the claims ... of the class'. Finally, the lead plaintiff must 'fairly and adequately protect the interest of the class'.

Once these requirements are met, then the class action must fall under one of the categories defined in Rule 23(b), which is commonly within the third category of claims for monetary damages (Rule 23 (b)(3)). This category requires that (1) questions common to the class must predominate over any questions that affect individual members of the class, and (2) class treatment must be 'superior to other available methods for the fair and efficient adjudication of the controversy.'[2] The final step, enunciated under Rule 23(c), directs the court to 'certify' the class once the case is filed to confirm that it can proceed as a class action.

While the origins of US class actions date well before the 1960s, the year 1966 marks a significant turning point, being the start of the modern era of class actions. It was in this year that the Federal Rules of Civil Procedure were amended so that members of a class action had to proactively 'opt-out' of a class action instead of 'opting-in', as was the case previously.[3] This development allowed for attorneys to launch class actions with no clients *per se*, using a single plaintiff to lead the case and regroup large numbers of members to the litigation, unless they proactively decided to leave the class action (which has proved rare in practice).

In the 1977 US Supreme Court case of *Bates v State Bar of Arizona*,[4] the Court ruled that attorney commercial advertising was protected as free speech under the First Amendment to the Constitution, effectively putting an end to bar ethics rules that prohibited such practices (recent developments are also now impacting bar ethics rules in France, with the *loi Hamon* that allows lawyers to advertise, with some restrictions[5]). This further opened the door for attorneys to more aggressively pursue not only class actions but also mass tort litigation.

As class actions took hold in US litigation culture, the effects were being felt due to the large settlement sums — often in the millions — which were generally perceived, at least by business interests, as having a negative impact on businesses and the economy in general. In one example, vaccine manufacturers would not have produced vaccines in the 1980s for fear of class actions had it not been for Congressional intervention.[6] As a result, recent years have been marked by efforts to curb the wave of class actions, either through legislative action, case law developments or dusting off old legislation to justify introducing mandatory arbitration clauses to preclude class actions.

To address the issue of judicial forum shopping, in which plaintiffs brought class action suit in the state having the most receptive state laws, Congress enacted the Class Action Fairness Act 2005[7], which allowed defendants to move national lawsuits to federal court if certain dollar thresholds are met. In the case of *Wal-mart v Dukes*, the US Supreme Court refused to certify as a class the claims that female employees had been victims of discrimination because their individual situations were too unique to qualify as a common class.[8]

More recently in 2011, in *AT&T Mobility v Concepcion*, the US Supreme Court held that private arbitration clauses that precluded class actions were enforceable under the Federal Arbitration Act 1925, essentially depriving consumers the option to join class action lawsuits to the delight of large corporations (and undeniably to the detriment of consumer rights) burdened by the class action sword of Damocles.[9]

Given this high-level procedural overview and historical context, one of the more noteworthy areas of recent growth in class actions has been in data privacy. While gaining traction in the wake of the Snowden revelations and general consumer privacy awareness that followed, privacy class actions have nevertheless been effectively checked by the difficulty of meeting Article III standing requirements imposed by the US Constitution manifested in recent case law.

Known as the *case or controversy* requirement, this rule requires a plaintiff to demonstrate injury-in-fact; the plaintiff must also show that the injury in question is fairly traceable to the defendant's challenged action; and the alleged injury must be one that could be redressed by a favourable judicial decision. The debate has been raging for years about how to show harm or injury for such incidents as a data breach, especially for a harm — through identity theft, for example — that may not occur until some unforeseen time in the future, if at all.

A recent US Supreme Court development has finally shed (some) light on the issue, marking a departure from some lower courts interpretations of what

constitutes harm to confer standing. In the 2016 case of *Spokeo, Inc v Robins*, the Supreme Court effectively limited the reach, albeit specifically in regards to the context of a procedural violation, of qualifying a harm caused by a privacy violation.[10]

The Court held, when considering whether a statutory violation (and one that does not result in concrete injury), that a plaintiff must suffer an injury-in-fact that is both particularised and concrete to have standing to sue, and that a 'bare procedural violation, divorced from any concrete harm' to the plaintiff cannot satisfy the injury-in-fact requirement of Article III.

To summarise the case briefly, Robins filed a class action against Spokeo, the operator of a people search engine, alleging violation of the Fair Credit Reporting Act 1970 (FCRA), and claiming that Spokeo 'wilfully failed to comply with the FCRA since the operator generated a profile containing inaccurate information about him'. While the Court stopped short of addressing if Robins had established a concrete injury, it did provide some indication of how to determine if an intangible injury is 'concrete' to qualify as an injury-in-fact to confer standing.

The legacy of Spokeo in the months after the decision has been mixed, with the question of conferring standing for intangible injuries being decided inconsistently by the courts.[11] In cases of data breach-related litigation, where the challenge has been to provide imminent risk of harm, the courts tended to confer standing.[12] On the question of unlawful disclosure of legally protected information protected by federal statute, the courts generally favoured interpretation that such an incident qualified as a concrete injury sufficient to confer standing[13] (although some courts took the complete opposite approach with similar facts[14]).

Taking a step back from *Spokeo*, not to mention the difficulty of qualifying a data breach or other privacy-related incident as sufficient to confer standing, the merits of class action for privacy offences can surely be questioned when looking at the larger impact of class actions in other areas. A study conducted by the law firm Mayer Brown,[15] while based on 2009 data, found that for the entire data set studied, not one of the class actions ended in a final judgment on the merits for the plaintiffs (none went to trial, either before a judge or jury) and the majority of cases produced no benefits to most members of the putative class (plaintiff lawyers instead reaping most of the financial benefits).

While the verdict is still out for how efficient privacy-related class actions are as a form of deterrent, the indications are that they are here to stay, especially as new technologies and social media practices continue to change the nature of what personal data are shared and in what capacity. US state laws have also been aggressively tightening privacy requirements for companies and public bodies — California being the most visible example — slowly approaching in some shape or form, and sector by sector (as inefficient and unwieldy as that has proven) — EU-style data protection laws.

CLASS ACTIONS FOR PRIVACY VIOLATIONS: ACROSS THE POND

While there are no common rules for class actions at the European Union (EU) level, thus creating any sort of pan-European harmonised approach to such litigation, the EU Parliament has provided recommendations on how to address the subject. Published on 12th February, 2012, the recommendation, 'To a Consistent Approach About Class Actions',[16] provided a first to step for a deeper analysis on how to create a harmonised or semi-harmonised approach across EU member states.

The European Commission, the 'executive' arm of the EU, then took the initiative in 2013 by producing its own recommendation, which essentially called on

individual member states to introduce class action procedure into their law.[17] While falling short of a harmonised approach, which would normally come in the form of a regulation or even a directive, the recommendation provided some guidelines, such as the prohibition of lawyers using contingency fees, as well as that of imposing punitive damages — two mechanisms that are key ingredients to the propagation of class actions in the USA.

In addition to the EU Commission guidelines and its markedly different conception of how class actions should operate across the EU, member states are unlikely to adopt US-style class actions anytime soon given their very different legal tradition. This difference is derived from the civil law tradition in the overwhelming majority of EU member states, in sharp contrast to the common law tradition of the USA (closely linked to that of the UK). Despite these inherent differences, the overall goal remains the same on both sides of the Atlantic: to enable better access to justice and facilitate the proof of damages.

CLASS ACTIONS *À LA FRANÇAISE*: A LITTLE OF THAT AND A LOT OF NOTHING

After much debate and analysis, class actions were finally introduced into French national law on 17th March, 2014, with the adoption of the '*loi Hamon*'.[18] The difficulty of adopting such a regime can be explained in part by the legal principle enshrined historically in Articles 30 and 31 of the French Civil Code of Procedure, summarised by the adage of '*Nul ne plaide par procureur*', essentially forbidding mandating a third party to litigate on one's behalf. This provision made any sort of class action in which one party represents an entire class of plaintiffs nearly impossible in French civil procedure.

The original *loi Hamon* limited the scope of class actions, making them possible only in the areas of consumer law and competition violations.[19] The legal landscape quickly evolved a few years later by expanding the class action scope to health,[20] environment,[21] workplace discrimination[22] as well as data privacy[23] (as will be explained in more detail below). With the exception of class actions involving consumer and competition violations, class actions are governed by the same procedural base. Indeed, Article 60 and subsequent articles of the Law for a Justice of the 21st Century (adopted 18th November, 2016) applies to all these class actions, including data privacy cases.

It is helpful to take a deeper look at the procedural aspects, which deviate significantly from those in the USA, revealing the limits of class actions in France. First, Article 62 of this law defines what situations can lead to a class action and which actions are targeted. To introduce a class action, persons must (1) be placed in the same situation and (2) suffer a damage caused by the same person whose common cause is a similar breach of (a) its legal obligations; or (b) its contractual obligations.

The class action can be initiated to obtain a court-ordered injunction to cease the action in question or to engage the liability of the person causing the damage in order to obtain compensation (a provision that does not apply to privacy-related class actions).

Where the procedural requirements begin to go off the rails is in their requirement that only certified associations and associations regularly constituted for five years, and whose statutory purpose is the defence of a prejudice, can initiate class action litigation (Article 63). The action can be introduced after addressing a formal notice to the future defendant to stop performing the activity in question or repair a damage. If this notice is unanswered after four months, only then can formal litigation proceedings be started (Article 64).

When the group asks for the cessation of a violation, the judge, if he agrees with

the claim, will order the defendant to stop it within a specified time (Article 65) and can also issue penalties. The judge will pronounce a statement about the liability of the defendant (Article 66 and subsequent articles) when the group asks for compensation. The decision must define the group, criteria to be part of the group, damages which can be repaired for each category of person in the group, the form of advertising and the time people have to join the group.

In comparison with the US model, the French class action is an opt-in class regime: a concerned party is not by default part of the group unless the party proactively joins. This requirement is also common to most class action procedures in EU member states (an exception to the rule will be discussed below).

The lack of efficiency of French-style class actions is also due in large part to the limited role of lawyers. Not only are they kept on a leash, unable to initiate class actions — this is left to government-certified associations — attorneys do not investigate the allegations *per se*, and cannot receive proportionate fees for their time. It is hard to imagine any class actions existing in the USA with such stringent requirements. While the procedure for consumer litigation is based on a different legal text, the requirements are generally similar.

Since 2014, only eight class actions have been introduced in France and most of them deal with telecommunications-related violations and against landlords of social housing. The lack of interest in class actions can be explained by many reasons, as alluded to above. According to a 2014 report entitled, 'Information Report about the Application of the *Loi Hamon*',[24] the novelty of the mechanism is not the only reason.

It was no surprise that the report concluded that the conditions to introduce a class action are too restrictive. While wanting to curb the potential for abuse from overly ambitious lawyers, lawmakers failed to realise that very few associations can actually introduce class actions due to their limited number, not to mention the cost of doing so, which is generally prohibitively expensive.

In practice, only one or two associations actually have the resources to finance a class action. Moreover, the procedure, as described in part above, is long and restrictive. It is complex to measure and prove a minor individual damage or breach of an undertaking. Finally, the report points out the existence of another related form of litigation, which is close to the class action, namely the 'joint representation action',[25] which can be introduced more easily and is often a better option. The report timidly suggests opening the action to other associations and even public authorities and to create a supporting fund to help financing actions.

THE GDPR: OPENING THE DOOR TO CLASS ACTIONS FOR PRIVACY VIOLATIONS

The class action regime for privacy violations began to appear in the recently-adopted General Data Protection Regulation (GDPR)[26] and, even before it officially comes into effect, provisions were introduced for privacy class actions in France (as will be detailed in the next section). At the EU level, the GDPR lays the foundation for what some claim to be privacy class actions. It is worth dissecting a few of the pertinent articles.

Article 80, entitled 'Representation of data subjects' states that:

> 1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a member state, has statutory objectives which are in the public interest, and is active in the field

of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by member state law.

2. Member states may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that member state, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

According to the first paragraph of the text, the data subject can mandate one of the three entities listed to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, exercise the right to receive compensation referred to Article 82 on his or her behalf where provided for by a member state law.

Article 77 of the GDPR recognises the right, for the data subject, to lodge a complaint with a supervisory authority (such a right already exists in France). As explained in more detail below for France, this mechanism permits the data subject to complain to the CNIL if the data subject considers that the processing of personal data relating to him/her infringes his/her rights.

Article 78 of the GDPR grants the data subject the right to an effective judicial remedy against a supervisory authority. The data subject can contest the decision of a supervisory authority pronounced against him or her. Finally, Article 79 of the GDPR states the right of the data subject to an effective judicial remedy against a controller or a processor.

Therefore, Article 80 (1) of the GDPR admits the possibility, for a not-for-profit body, an organisation or association, mandated by a data subject to exercise all the rights listed above. The mandated body can also receive compensation on behalf of the data subject. Article 82, concerning the right to compensation and liability, states that 'Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'.

This is a new possibility offered to data subjects to mandate a legal entity to represent him or her in most member states. Indeed, some see the beginnings of a pan-European class action regime for privacy violations. While this is a bit of stretch, it does allow for some resemblance of collective litigation, permitting each person to mandate an association to act on his or her behalf.

DATA PRIVACY CLASS ACTION IN FRANCE: LAUDABLE OR LAUGHABLE?

Following on the heels of the GDPR adoption, on 18th November, 2016, France introduced a law permitting a class action to be introduced when a group of natural persons, in a similar situation, suffer damages due to a violation of data privacy.[27] The law is aimed at data controllers as well as data processors, which is consistent with how the soon-to-take-effect GDPR views their respective liability.

There are some peculiar aspects to the new law, however, which will likely ensure that privacy class actions never see the light of day. The most blatant shortcoming is that a privacy class action can only lead to a court-issued injunction to terminate the action in question, with no compensatory damages. Moreover, only three kinds of

organisations can introduce such an action, including:

- association regularly constituted for five years whose statutory object is to protect privacy and personal data;
- consumer protection associations when the process affect consumers; and
- trade unions when the process affects the interest of a person under its mandate to represent.

The introduction of class actions in France was the brainchild of the Conseil d'Etat (a high-level French government advisory body), dating from its 2014 annual report entitled 'Digital Technologies and Fundamental Liberties'.[28] While at first glance this initiative, essentially based on the same principles as the other class actions in France (including the same procedural rules) is laudable, intended to increase the protection of data subjects and better protect their rights, it falls horribly short for rather obvious reasons, some of which have already been evoked above.

First, the qualified associations that are able to initiate such class actions are too few in number, most of them established well before the required five-year benchmark. To make matters worse, litigation can only be introduced after a period of four months once a formal notification is made to the future defendant. In contrast, a complaint made to the French Data Protection Authority, La Commission Nationale Informatique et Libertés (CNIL), will most likely result in some form of action within two or three months from the date the complaint is filed.[29] So, if the goal is to seek a termination of the action in violation of data protection law, it is more efficient simply to file a complaint to the CNIL instead of waiting four months to initiate a complex procedure to achieve the same result.

It gets worse. The class action suit can only result in termination of the action in question and not any form of compensation. In addition, the judge is not able to render public the data protection violation, essentially depriving the plaintiff of another potential stick for publicly shaming the other party. The privacy class action procedure, however, is still an unfinished legislative process according to the Senate *rapporteur*, who plays a key role in drafting and adopting legal texts in the Senate, who completed an insightful report in 2016 focusing on the shortcomings of privacy class actions.[30]

The *rapporteur* highlights several points in his report: first, a class action based on a violation of data protection law is in practice less effective than litigation based on a defence of a collective interest as this option does not require constituting a group. This option allows an association to initiate litigation independently (but for the moment is permissible only for consumers, for example, in cases of abusive clauses in consumption contracts). Furthermore, the *rapporteur* considers it paradoxical to base an action for the cessation of a breach on the precondition of injury whereas the action does not provide for the compensation for that damage. He concludes with the obvious statement that that the new class action regime for privacy is essentially symbolic in nature and does not present real added value for data protection.

The *rapporteur* is not alone in his conclusions. The challenge in tweaking the law to permit compensatory damages shares the same complexity that has resulted in the current legal tension in the USA: how does one effectively qualify and measure the intangible damage caused by a privacy violation?

Class actions for data privacy violations also have another peculiarity. In a departure from the current EU Directive 95/46/EC on data protection, the new GDPR will allow litigation to be initiated due to

violations committed by the data processor as well as data controller. In fact, current French law has already been updated to include this GDPR provision, providing for equal liability for both data processors and data controllers.[31]

A recent case dating from 9th February, 2016 now allows trade unions the right to exercise all the rights reserved to the civil party in respect to acts constituting a violation of the French Data Protection Act 1978 (in this case, lack of reporting of a video surveillance system) directly or indirectly harming the collective interest of the profession they represent.[32] Class actions seem destined to take a back seat in French law when it comes to violations of data privacy.

It remains to be seen how the GDPR will further influence the class action regime in France. Article 82 of the GDPR, for example, states that the data subject shall have the right to compensation for a damage suffered. A class action can be introduced when several persons are in the same situation and have suffered the same damage because of the same person. Therefore, to comply with Article 82, French privacy-related class actions should allow for the compensation of damages unless one considers that this compensation was meant to result from individual litigation only.

The question is always the same: how to calculate a potential damage? In sharp contrast to the USA, there is no case law in France providing any guidance for the moment. Furthermore, the French are generally litigation-shy in such matters, preferring instead to file complaints to the regulatory authority.

While the GDPR falls short of creating a dedicated regime for privacy-related class action in EU member states, it nevertheless provides the possibility for data subjects to mandate an organisation to act on their behalf. This may be the start of greater things to come.

A CLOSER LOOK: CLASS ACTION FOR PRIVACY VIOLATIONS ELSEWHERE IN EUROPE

As explained above, there is no harmonising regime for class actions in the EU, essentially allowing EU member states to legislate as they see fit in the matter. It is worth taking a detour to Austria simply because it is the jurisdiction where the most well-known privacy class action has been initiated to date, started in August 2014 by Maximiliam Schrems.[33] The case takes aim at Facebook (Ireland) and is still working its way through the courts.

Austrian law permits, as part of a common damage involving several people, to mandate a party of that group to go to court on behalf of the others. The designated person is the main plaintiff, representing all the others. If damages are awarded, the plaintiff must transfer them to each member of the group. In practice, each member of the group gives their claim for compensation to the plaintiff who represents the group.

In the case against Facebook, some 25,000 individuals from all over Europe have joined Schrems in his claim, each asking for €500, making a total claim of €12.5m. Interested parties can still join the class action if concerned by the action but will not receive damages. The plaintiff has presented a long list of claims: (1) Facebook's policy on the use of data does not comply with European laws; (2) Facebook has not obtained consent for many of the ways it has used the data; (3) Facebook provides data to the National Security Agency's PRISM programme; (4) Facebook monitors users on external websites; (5) Facebook leverages Big Data to monitor and analyse users' behaviour; (6) the introduction of Facebook's Graph Search was illicit; and last but not least, (7) Facebook transmitted data to external applications without authorisation.

There are many questions at stake in this case. Is it possible for Schrems to represent European plaintiffs (or only Austrians)? Is he a consumer? These questions have been

referred to the European Court of Justice by the Oberster Gerichtshof (Austrian Supreme Court) in a request for a preliminary ruling.[34]

Facebook has taken the offensive by asserting that an Austrian can only initiate a class action made up exclusively of Austrian nationals. The company also argues that Schrems cannot be considered as a consumer (ie someone who has concluded a contract for a purpose which can be regarded as being outside his trade or profession[35]). Facebook holds that Schrems used his Facebook account to promote his legal agenda, sell books in connection with the enforcement of his claims, collect donations for the enforcement of his claims and advertise for meetings. According to Facebook, he must be considered as a professional, and therefore cannot benefit from the choice of jurisdiction offered to consumers in Article 15 Regulation Brussel 1.

In the torrent of arguments made by Facebook, the primary objective is to obtain the incompetency of the Austrian jurisdiction in favour of Irish courts and therefore to declare the class action impossible. Facebook wants to split pleas and relocate the action in far-off Ireland — an effective way to demotivate plaintiffs.

The European Court of Justice could decide in a variety of ways. It can decide that Schrems is a consumer and therefore recognise the jurisdiction of the Austrian courts, given that a consumer has the right to use the legal system where he resides in order to sue a professional. The court can also decide that Schrems must be considered as a professional and, therefore, the Irish courts will be competent.[36]

The European Court of Justice must also decide on the possibility for a consumer to represent others regarding the Regulation Brussel 1. Four scenarios are therefore possible:

- The European Court refuses the possibility of introducing a class action within the scope of Brussel 1. This would seem particularly unfavourable to consumers, as they would be obliged to sue a professional on their own. Asserting their rights would be difficult.
- The European Court recognises class actions, but restricts them to citizens of the same country. This solution is not ideal as not all countries have a class action regime, hence some citizens would be in more favourable positions than others.
- The European Court of Justice accepts that a class action may gather citizens from different member states. This could result in a new kind of European class action, with plaintiffs effectively shopping to find the member state with the most favourable class action procedure and judge. This solution could lead to the EU adopting a common class action procedure.
- Finally, the Court accepts that a class action may gather citizens from any country, as long as one of them is from an EU member state. This solution is particularly unfavourable to professionals and could have a terrible effect on the European market.

While the second or the third solution seem most plausible, whatever happens, the outcome of the Schrems case will have significant repercussions throughout Europe and may very well result in the class action regime being redesigned.

A LOOK AT ENGLAND AND WALES, PORTUGAL AND SPAIN: A SIGN OF THINGS TO COME

It is helpful to look at the a few other EU jurisdictions in addition to France and Austria as such an analysis provides insight into how class actions may evolve throughout the rest of Europe. In the case of England and Wales, class actions have existed since the Middle Ages, but were reintroduced at the end of the 20th century. They permit individuals to initiate legal action through a single lawyer and can be

introduced to recognise their rights, claim damages and include compensation; they can also apply to all civil actions, not just those in specific legal sectors.

There are two main procedures to consider: group litigation orders and representative actions. Group litigation orders allow group judicial actions to be initiated that raise common or related questions of fact or law.[37] Classical rules of procedures apply. The judge must deliver an authorisation to create a class action at the request of one of the parties who already went to court in an individual capacity. A solicitor is required to be the key contact for the entire group — another marked difference compared with the French model.

A class action must ensure that each party can present its case and defend itself, and permits similar cases to be treated in the same way. Today, England and Wales have two kinds of class actions: opt-in class actions and opt-out. The opt-out mechanism, resembling that of the US, is relatively new and was introduced by the Consumer Rights Act 2015. It is limited in scope, only allowing consumers to obtain compensation when companies fix prices or form cartels. It concerns two kinds of procedures:

- *follow on:* introduction of the action after a decision of the competition authority; and
- *standalone procedure:* going to court independently of a decision of the competition authority to recognise a violation of competitive law.

While privacy class actions are not specifically addressed in the law, it would be entirely feasible for people suffering the same damage to initiate a collective action.

In contrast, Portugal has included class action litigation as a fundamental right as part of Article 52 of its constitution. A law dating from 31st August, 1983 defines the procedure.[38] The class action procedure is large in scope and can be initiated by any citizen, an association or public prosecutor. The aim of the action can be preventive, declarative, restorative or executory. It is possible to ask for redress or cessation of unlawful conduct.

Spain also has its own form of class action — the *Ley de Enjuiciamiento civil.* The law provides for three different types of interest: general, collective (consumers are victim of the same identified damage) and diffuse (consumers are victims of the same damage but their identity is not known). Persons qualified to act are different according to the type of interest involved.

It seems that a class action introduced on the behalf of a diffuse interest is an opt-out class action but it is difficult to determine as class actions are so rare in practice.

While different forms of class actions exist in different EU jurisdictions, some resembling the US regime (like in England, Wales and Portugal) while others (most obviously, France) are literally in a class of their own, the landscape continues to evolve quickly. Privacy-related class actions hold the most potential for rapid evolution notwithstanding the inherent difficulty in qualifying harm.

Even if EU case law is scarce, the outcome of the Schrems case, as well the developments of case law in the US, could signal greater appetite for Europeans to litigate in the form of a class action. For the moment, however, the greatest threat to large companies operating in Europe that violate data privacy law comes not from the risk of class action litigation but instead from EU regulators who will be newly endowed with impressive sanctioning powers when the GDPR takes effect in May 2018.

References

1. Alexander, J.C. (2000) 'An Introduction to Class Action Procedure in the United States', conference paper presented at Debates over Group Litigation in Comparative Perspective, Geneva, Switzerland, 21st–22nd July; For additional detail regarding

Rule 23(b)(3) of the Federal Rules of Civil Procedure, see *Amchem Products, Inc. v Windsor*, 117 S.Ct. 2231 (1997).
2. Alexander, ref. 1 above.
3. See Fed. R. Civ. P. 23(c)(3)(B).
4. *Bates v State Bar of Arizona*, 433 US 350 (1977).
5. Article 3 *bis de la loi no. 71-1130* of 31st December, 1971, complemented by *la loi no. 2014-344* of 17th March, 2014 *relative à la consommation*, otherwise known as the *loi Hamon*.
6. See National Childhood Vaccine Injury Act 1986, 42 USC § 300 (2004); see generally, Burke, T.F. (2002) 'Lawyers, Lawsuits, and Legal Rights: The Battle over Litigation in American Society', University of California Press, Berkeley, CA, pp. 142–170.
7. Pub. L. 109-2, 119 Stat. 4-14.
8. See *Wal-Mart Stores, Inc. v Dukes*, 564 US 277 (2011).
9. *AT&T Mobility v Concepcion*, 563 US 333 (2011); *American Express Co. v Italian Colors Restaurant*, 570 US, 133 S. Ct. 2304 (2013).
10. *Spokeo, Inc. v Robins*, 136 S. Ct. 1540, 1545 (2016).
11. See further analysis in Southwell, A.H., Vandevelde, E., Bergsieker, R. and Maute, J.B. (2017) 'Gibson Dunn reviews US cybersecurity and data privacy' in Gibson, Dunn & Crutcher LLP (2017) 'US Cybersecurity and Data Privacy Outlook and Review: 2017', memorandum, 27th January, available at: http://www.gibsondunn.com/publications/Pages/US-Cybersecurity-and-Data-Privacy-Outlook-and-Review--2017.aspx (accessed 30th June, 2017).
12. *Galaria v Nationwide Mut. Ins. Co.*, Nos. 153386, 2016 WL 4728027, at *6 (6th Cir. Sept. 12, 2016); *Lewert v P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 970 (7th Cir. 2016).
13. In *re Nickelodeon Consumer Privacy Litig.*, 827 F. 3d 262, 273–74 (3d Cir. 2016).
14. For example, *Noble v Nev. Checker CAB Corp.*, No. 2:15CV02322RCJVCF, 2016 WL 4432685, at *4 (D. Nev. 19th August, 2016).
15. Mayer Brown LLP (n.d.) 'Do class actions benefit class members? An empirical analysis of class actions', available at: http://www.instituteforlegalreform.com/uploads/sites/1/Class_Action_Study.pdf (accessed 30th June, 2017).
16. European Parliament, 2nd February, 2012, no. 2011/2089.
17. European Commission, 11th June, 2013, no. 2013/396/UE.
18. Loi no. 2014/344 du 17 mars 2014 relative à la consommation.
19. Articles L623-1 et seq of the Consumer Code.
20. Loi no. 2016-41 du 26 janvier 2016.
21. Article 60 de la loi no. 2016/1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.
22. *Ibid.*
23. *Ibid.*
24. Rapport d'Information de la Commission des affaires économiques de l'Assemblée nationale sur la mise en application de la loi no. 2014-344 du 17 mars 2014 relative à la consommation.
25. 'Action en représentation conjointe' and Articles L622-1 et seq of the Consumption Code.
26. Regulation 2016/679 of the European Parliament and of the Council of 27th April, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
27. Article '43 ter' introduced the French Data Protection Act 1978 — Loi informatique et libertés no. 78-17.
28. Conseil d'Etat (2014) 'Etude annuelle 2014 — Le numérique et les droits fondamentaux', available at: http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-etat-le-numerique-et-les-droits-fondamentaux (accessed 30th June, 2017).
29. For example: Decision no. 2016-058, 30th June, 2016/Decision no. 2016-079, 26th September, 2016.
30. Senate Report no. 839 (2015-2016), 21st September, 2016, p. 132.
31. Article 28 of Regulation no. 2016/679.
32. Supreme Court, 9th February, 2016 — Cour de cassation, chambre criminelle, 9 février 2016, no. 14-87.753.
33. Schrems is well known for having initiated the case that led to the invalidation of Safe Habor: CJUE, 6th October, 2015, C-362-14, Maximilian Schrems/Data Protection Commissioner.
34. Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 19th September, 2016 — *Maximiliam Schrems v Facebook Ireland Limited* (Case C-498/16).
35. Article 17 of Regulation Brussel 1 bis.
36. Articles 2 and 5 Regulation Brussel 1.
37. Part 19 Section 3 of the Civil Procedure Rules.
38. Law no. 83/95 from 31st August, 1983.