Going global: Data class actions make their way to the EU

10 December 2018

Class actions have become an increasingly common means to seek redress in data privacy cases. With data breaches and data privacy claims on the rise, we asked our lawyers in France and the U.S. what you should bear in mind.

How real is the risk of class actions in data privacy?

Michelle Kisloff, U.S.: Class actions have long been a fact of life in the U.S., in areas ranging from securities, product liability, employment and consumer protection, to name a few. For the past several years, they have been on the rise in data privacy. So yes, it's a real risk.

Christine Gateau, France: Data privacy breaches usually affect lots of people. One person's claim may be too small to launch an action on its own, generally. This makes class action — the opportunity to bring joint claims — a stronger option. Plus, French lawmakers are in favor of allowing consumers to seek redress for data loss and privacy breaches.

Adam Cooke, U.S.: The risk is real. But in the U.S. plaintiffs have hurdles to overcome in prosecuting a class action. A threshold hurdle is that plaintiffs must show they have the ability, or "standing," to bring a claim. One component of standing is injury, and plaintiffs must show they have suffered or will suffer losses, which must be real or imminent, not hypothetical. The mere possibility of future harm alone is not enough.

With this in mind, what should you be aware of?

Christine Gateau, France: Companies are more engaged with the idea of data class actions now that the General Data Protection Regulation (GDPR) is in force. Speaking to our clients having become compliant, they're keen to know what to do to stay one step ahead.

Companies should be aware that the GDPR exposes them to a two-pronged approach to action. Claimants can appoint an authorized entity to bring an action or to claim compensation. Or if allowed in the Member State, the entity can act without being appointed.

Is there a trend in the outcomes of these class actions?

Michelle Kisloff, U.S.: We've seen different outcomes in the U.S. The federal courts of appeals have split over whether plaintiffs have standing based on alleged increased

risk of future fraud and identity theft. Lower courts are similarly divided. It depends on the facts of each case.

Adam Cooke, U.S.: The Second Circuit's opinion in *Whalen v. Michaels Stores*, Inc., is a good example. In this case, the named plaintiff alleged her stolen credit card data was used to make bogus payments, but she also quickly cancelled the card and was never liable for any unauthorized payments. The court found that the plaintiff lacked standing. These cases do turn on the underlying allegation and facts. We expect a clearer picture of trends to emerge as more cases move through the courts, or if the U.S. Supreme Court weighs in.

What are some of the pitfalls of the U.S. regime?

Michelle Kisloff, U.S.: It's not clear that class actions are a good fit for the types of injuries alleged in these cases. Even if a data privacy class action survives multiple challenges, there's often no actual loss to recover, so no damages can be awarded. Plaintiffs are seeking to put a common monetary figure on things like the value of keeping certain information private. But the evidence shows that different people value their privacy differently. Because of the reach of websites and mobile apps, data class actions often involve tens of millions of class members. This can make the cases difficult to resolve and very expensive to defend.

Also, for class actions based on data security and privacy, there's no clear national standard. Instead, there's a patchwork of federal and state laws, some of which were created for different purposes. The Computer Fraud and Abuse Act, for example, addresses computer-related activities. But it was aimed at malicious hacking. Under the statute, a plaintiff must allege at least US$5,000 in damages, which many plaintiffs in data privacy class actions simply cannot do.

Adam Cooke, U.S.: Many privacy class actions that are not dismissed are resolved through settlement. And these settlements often return minimal benefits to the class members. Some do not include any direct monetary payments. Instead, they require defendants to make payments to charitable organizations that indirectly benefit the class. Other settlements provide certain services like free credit monitoring.

Could the EU also end up with a patchwork of national laws?

Christine Gateau, France: The GDPR enables claims in national courts. It doesn't create a European class action; this is left to each Member State. This means we could see different collective action procedures in different countries.

Under the GDPR, someone whose personal data has been compromised or used in a non-compliant way can claim both material and non-material damages, depending on the law of their Member State. This is an important difference from the U.S. regime, and it increases the possibility for claimants to bring a class action in the EU.

What issues might you experience as a result in the next few years?

Christine Gateau, France: It doesn't follow that EU data subjects[1] will get high damages. In some Member States, there is an entitlement to material and non-material damages, yet it's hard to put a figure on non-material damages. For instance, what's the value of anxiety from knowing your credit card details have been stolen, if there's no financial loss?

Each EU Member State could decide to put in place something similar to the U.S. charity payments. But this has its own issues — giving money to an association doesn't achieve the GDPR's goal of compensating the data subject. And if compensation is likely to go to a third party, affected data subjects may not join the class.

Michelle Kisloff, U.S.: Class action hasn't established widespread standards in data privacy because so few disputes have gone to the merits for decision. But we have seen increased regulatory action in the U.S. And both the U.S. Federal Trade Commission and various state attorney generals are pursuing enforcement actions to try to set certain standards for others in the market to follow. Typically, resolutions of these actions include terms aimed at addressing the activities that led to the complaint and have seen defendants ordered to change their policies. It's worth monitoring the Commission's enforcement actions against other companies and considering updates to your processes and policies in light of those actions.

And is there a potential wider effect?

Christine Gateau, France: Recoverable loss may be defined differently across the EU. And some national courts may be more likely than others to grant damages. It's possible this could lead to forum shopping in the EU.

Adam Cooke, U.S.: Disparate outcomes in class action litigation could create incentives for plaintiffs to "forum shop." If a court issues a decision favorable to plaintiffs on a question of, say, standing, it's reasonable to expect future plaintiffs may try to start litigation in that particular court.

Christine Gateau, France: Another possibility we may see is class actions launched in various countries. You would then need to be prepared to defend across countries and to comply with various national procedural rules around discovery and document access.

Data protection authorities have different styles. Some will use all investigatory powers — almost equal to discovery — granted by the GDPR. Associations could then use information gained this way to launch a data class action. Investigations may last a few months. So you could face a risk of disruption — and of reputational damage.

What can you do to protect yourselves against the threat of data class actions?

Christine Gateau, France: The data class action coordination mechanism is new to both companies and data protection authorities — everyone's learning. We're seeing data protection authorities use caution. They don't want to apply their powers in a

way that might be contested.

If an authority wishes to investigate your business, there's little you can do to stop it. But you can take steps to minimize the associated cost and disruption. Most important is to make sure you comply with the GDPR.

Keep hold of documents and records so you can cheaply and easily respond to requests for information. Have your privacy impact assessments ready. Appoint a data protection officer if this is appropriate for your organization. And work to establish good relationships with the data protection authorities.

Michelle Kisloff, U.S.: Prevention and preparation are always the places to start. Make sure you have a global data breach response program that varies, as needed, by jurisdiction. Know your reporting obligations in each jurisdiction both to authorities and to individuals. Plan for likely scenarios, the consequences of each, and the steps you'd need to take to mitigate the consequences.

Beyond this, know that if you have a data breach and litigation follows, you do have potential defenses. Where plaintiffs cannot show their data has been misused, courts should find that the class plaintiffs lack standing or injury. Even if a court finds plaintiffs do have standing at the pleading stage, there's often a great opportunity to challenge whether the plaintiffs have common, class-wide damages at class certification. At the end of the day, it can be hard for plaintiffs to prove they suffered any injury that was actually caused by the defendant. And of course, we advise companies to develop their narrative on the strength of their data compliance program on the merits.

You'll find more information in our European Privacy Tool , which walks you through how the GDPR affects your business. It includes practical steps to help you fulfill your obligations.

You should also read our guide *Data class actions: The era of mass data litigation*. It shares insights into class actions in the U.S and the EU, including Italy, Poland, Spain, the Netherlands, and the UK.

Contacts

Michelle A. Kisloff

Partner

Christine Gateau

Partner

Adam A. Cooke

Counsel

> Read the full article online