REPRINT

CD corporate disputes

DATA PROTECTION CLASS ACTIONS

REPRINTED FROM:

CORPORATE DISPUTES MAGAZINE

JAN-MAR 2021 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request a free copy of the full e-magazine

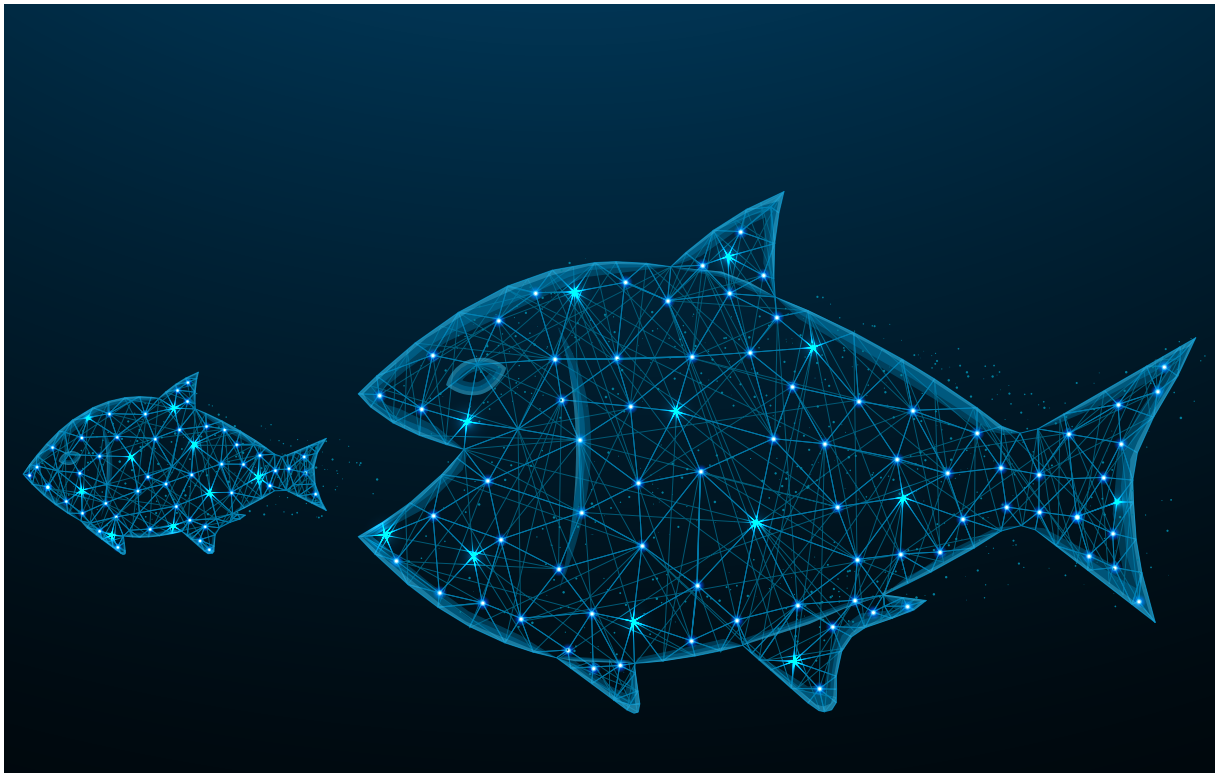
SHOOK HARDY & BACON

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

www.corporatedisputesmagazine.com

HOT TOPIC

DATA PROTECTION CLASS ACTIONS



PANEL EXPERTS

Alexis Collins
Partner
Cleary Gottlieb
T: +1 (202) 974 1519
E: alcollins@cgsh.com

Alexis Collins' practice focuses on complex civil and antitrust litigation, criminal and regulatory enforcement matters, and cyber security. Ms Collins first joined Cleary Gottlieb in 2001. In 2003, she joined the US Department of Justice (DOJ), where she served in numerous positions for more than a decade. She returned to Cleary Gottlieb as a senior attorney in 2015 and became a partner in 2019.

Kenny Henderson
Partner
CMS
T: +44 (0)20 7367 3622
E: kenny.henderson@cms-cmno.com

Kenny Henderson is an experienced litigator who represents sophisticated and blue chip clients in high stakes disputes, frequently with a multijurisdictional element. He is solutions-oriented and deploys litigation strategies tailored to deliver commercial objectives. He has particular expertise in regulated sectors, including pharmaceutical and technology claims.

Steven Hadwin
Director, Head of Operations – Data Protection, Privacy and Cybersecurity
Norton Rose Fulbright LLP
T: +44 (0)20 7444 2290
E: steven.hadwin@nortonrosefulbright.com

Steven Hadwin is a dispute resolution lawyer based in London focused on cyber risk management and incident response. He frequently advises clients on the legal implications, including under the GDPR and the NIS Directive, of adverse cyber incidents, including data breaches, malware attacks and network interruptions. Many of his clients face cyber risk issues in a range of geographies and he is experienced in co-ordinating the legal response to cyber incidents across a range of jurisdictions and regions.

Al Saikali
Chair, Privacy and Data Security Practice
Shook, Hardy & Bacon L.L.P.
T: +1 (305) 358 5171
E: asaikali@shb.com

As chair of Shook's privacy and data security practice, **Al Saikali** has gained the trust of clients challenged by data incident response, privacy litigation and compliance with the myriad laws governing sensitive information. He believes that client service, deep experience and proactive thinking are what separates him from other privacy and data security lawyers. These values are illustrated by the fact that Chambers USA ranked him Band 4 in Privacy and Data Security in 2020, and he was named a cyber security trailblazer by the National Law Journal in 2015.

CD: To what extent do data privacy and protection issues continue to present increasing risks for companies? How would you summarise the evolution of related laws and compliance obligations in recent years?

Collins: Data privacy and protection issues pose an ever-increasing risk, with cyber security breaches becoming a 'when, not if' conversation among chief information security officers (CISOs) and company executives. Lawmakers and government agencies in the US have responded to these risks with the continued adoption of fragmented data privacy laws and regulations. The patchwork of laws and regulations imposed by state and federal agencies has presented the opportunity for more government enforcement and claims by private parties but has also created compliance issues for companies.

Hadwin: Data privacy and protection issues continue to present new and increased risks to companies. Much has been written about the potential for large fines being imposed against data controllers for a failure to comply with their obligations under the General Data Protection Regulation (GDPR). While recent fines imposed by the Information Commissioner's Office (ICO) and other European data protection authorities have made this a reality, significant fines have been relatively rare – with only 14 fines in excess of €1m having been imposed across Europe since the GDPR came into force. Of perhaps greater concern here in the UK is the growth in litigation being brought post-data-breach by affected data subjects, particularly in respect of breaches material in size and sensitivity. While the per-claimant value of claims in this area tends to be low unless financial loss is alleged, controllers do face a risk of material costs and potential liabilities in the event that claims are brought by a large number of data subjects.

Saikali: As companies increasingly collect more information about their customers, employees, and business partners and find more ways to improve products and services through data mining personal information, the risks to privacy and data security will continue to rise. While it is difficult to paint the privacy landscape with a broad brush, the US approach, until recently, was fairly 'reactive' – requiring notice after there has been an incident. That is starting to change, as we saw with the recent enactment of the California Consumer Privacy Act (CCPA), which takes a more GDPR-like approach to privacy. In contrast, Europe has taken a more 'proactive' approach – imposing obligations on organisations to think about privacy from the inception of developing products, services and systems. But Europe's incident response regulations, which require notice within 72 hours and limit data transfers to countries whose government has essentially the same level of access to personal

information as European governments, are not practical. So, there is probably work to be done under both models.

Henderson: The clear trend is that risk from privacy and data protection issues is increasing. The introduction of the GDPR in 2018 materially increased the risk of non-compliance with data protection regulations, bringing the potential for significant fines of up to €20m or 4 percent of annual turnover. The recent wave of data protection class actions adds a new, and very significant, dimension of risk.

CD: How would you describe recent data protection class action activity? Are case numbers rising?

Hadwin: Claimant law firms are increasingly seeking group litigation orders (GLOs) or pursuing representative actions. Such law firms, and their funders, are doing an effective job of signing up claimants following large data breaches, on a conditional fee arrangement (CFA) basis. Claimants participate in claims without assuming material costs risk and, in many cases, without having to directly participate in proceedings. As well as the work being done by claimant law firms and third-party funders, a societal shift in consumer perception does appear to be contributing to this increase. It appears to be the case today that members of the public have higher expectations in relation to the personal data which they provide to companies, particularly in terms of those companies keeping that data secure. When those expectations are not met, there does seem to be an increased willingness on the part of some – certainly here in the UK – to seek redress.

Saikali: The numbers are definitely rising, but more significantly, the basis for the lawsuits is becoming far more diversified. For example, most of the privacy class actions in the US, until the last year or two, arose from data breaches and involved allegations that the breached entity failed to adopt reasonable security safeguards to prevent the breach from happening. Now we are seeing more of those lawsuits as a result of the CCPA's right to statutory damages, but we are also seeing other kinds of lawsuits where statutory damages may be a possibility, such as the Illinois Biometric Information Privacy Act (BIPA), which has spawned hundreds of lawsuits over the last few years. Additionally, we are seeing lawsuits based on allegations that consumers were not clearly informed about how their data would be collected, used and shared. This trend will continue as more states adopt laws that create private rights of action for privacy and security violations, and as companies find new and innovative ways to use and share personal information.

Henderson: At present, claimant law firms and litigation funders are very focused on data protection class actions in the UK; potentially even more so than their traditional hunting grounds for class actions, such as antitrust and product liability. In the past few years, there has been an uptick in large claims filed using 'opt-in' mechanisms. But the real story in the UK is the developing availability of an 'opt-out' mechanism for bringing data protection claims, predicated on *Lloyd v. Google*. This mechanism allows a representative to bring a claim on behalf of a huge number of class members, without needing to persuade them to join the claim. 'Opt-out' mechanisms are therefore extremely powerful devices for coalescing classes – the recent claim filed against YouTube is reported to encompass a class of five million. It would not have been possible to bring this claim on an opt-in basis.

Collins: Class action activity regarding data protection violations is increasing across US jurisdictions. This is partially being spurred by the continuing increase in data breaches that result in the exposure of consumer or employee information, as well as an increased focus by the plaintiffs' bar on the data privacy practices of consumer-facing companies. It also is a result of the adoption of privacy laws in certain states that permit private rights of action, such as the Illinois BIPA and the CCCPA.

> **"It appears to be the case today that members of the public have higher expectations in relation to the personal data which they provide to companies, particularly in terms of those companies keeping that data secure."**
>
> *Steven Hadwin, Norton Rose Fulbright LLP*

CD: What are the potential sources of a data protection class action? Are you seeing any common themes?

Saikali: There are three primary sources of a data protection class action. First, data breaches. This involves allegations that the company failed to adopt reasonable security safeguards to prevent a breach from occurring. Second, statutory violations. Certain state privacy laws, like the CCPA and the Illinois BIPA, create private rights of action and allow for certain statutory damages, which makes it easier for plaintiffs to overcome their otherwise biggest hurdle – standing. Finally, unauthorised collection or sharing. Companies are increasingly

collecting information about consumers and users and then sharing that data with third parties to improve services or otherwise monetise the data. The lack of transparency as to some of this behaviour has led to an uptick in privacy lawsuits that seek violations under state consumer protection laws, negligent misrepresentation claims, and breach of written and implied contract.

Collins: The most common causes of data protection class actions are the occurrences of a cyber security breach that results in the exposure or theft of sensitive personal information belonging to consumers, or a company's alleged failure to accurately disclose its data collection and sharing practices or to implement reasonable cyber security measures. BIPA class actions tend to focus on the failure to disclose the collection and use of biometric data. Another interesting trend to watch will be the result of the increase in data breaches resulting from the sudden and large shift to remote work brought on by the coronavirus (COVID-19) epidemic, and whether any increased litigation occurs as a result.

Henderson: In recent years, large data protection class actions brought on an opt-in basis have focused on data breaches, with the class seeking damages for pecuniary losses or distress. The recent series of opt-out class actions filed in England includes a data breach claim – *Marriott International Inc. Customer Data Security Breach Litigation* – but other claims are seeking damages on data protection issues beyond breaches, such as the claim against YouTube that contends that the consent given by the class of 13-year-olds and younger was ineffective in law. The expansion of class actions beyond data breaches is deeply concerning; claimant law firms do not need to wait for the 'black swan' moment of a data beach. They are exploring usages of data that arguably breach regulations, irrespective of whether a regulator has found an infringement. Relatedly, opt-out mechanisms create an acute 'rush to the courthouse' dynamic which encourages claims to be filed ahead of regulatory activity.

"The expansion of class actions beyond data breaches is deeply concerning; claimant law firms do not need to wait for the 'black swan' moment of a data beach."

Kenny Henderson, CMS

Hadwin: In relation to the causes of action being pleaded, in the context of a malicious cyber attack against a company, claimants are typically asserting that any breach of a controller's information security systems equates to a breach of that controller's security obligations under the GDPR, and any misuse of personal data by a malicious third party should be imputed to the controller itself, thereby also constituting a breach of the controller's obligations under the GDPR. Other causes of action which are often pleaded by claimants in claims of this kind include tort claims for misuse of private information and equitable claims for breach of confidence.

CD: Have there been any recent, notable data protection class actions? What were the key take-aways from these cases?

Henderson: The most significant recent claim in this space is *Lloyd v. Google*. This claim was brought under the longstanding English 'representative action' procedure that permits a representative to bring an opt-out claim on behalf of a class provided that the representative and the class members have the "same interest" in the claim. The English courts have historically policed the "same interest" test tightly and rejected many efforts to bring representative actions, and so this device has been considered ineffective and has rarely been used in recent years. Mr Lloyd is bringing the claim on behalf of an estimated 4.4 million iPhone users who he contends had their data protection rights breached by Google's alleged gathering of browsing behaviour over a period of six months. In allowing the claim to proceed, the Court of Appeal made two key findings. First, that "loss of control" of their data in of itself entitled the class members to damages. Second, the class members had the "same interest" in the claim and that accordingly use of the representative action procedure was permissible. Availability of an opt-out device for these types of claims is a major development and materially increases the risk profile of companies that may be targeted. *Lloyd v. Google* is on appeal to the Supreme Court which may reject use of the representative action device.

Hadwin: The *Lloyd v Google* Court of Appeal judgment, which is subject to appeal to the Supreme Court, is certainly the most notable case at present. Of most relevance, claimants are relying on the finding that loss of control of personal data can itself equate to compensable damage. The decision as it currently stands is also being challenged by defendants on the basis that the finding relates only to personal data which has inherent economic value, and, in any event, a *de minimis* threshold needs to be met before damage of any nature can be established. The Supreme Court hearing is likely to provide some degree of clarity in this area.

Collins: There have been a number of notable cases in the past two years. Several cases ease

plaintiffs' ability to sue over data breaches. For example, in February 2020, in *Marriott*, a district court found that consumers whose personal and financial information had been stolen in a data breach but had not suffered identity theft had standing to sue in part because they had lost the value of their personal data as a commodity. The court recognised that data is increasingly valuable in the digital economy and held that its theft deprives individuals of the value of their data. Additionally, the Seventh Circuit Court of Appeals bolstered BIPA plaintiffs' ability to establish standing to sue in *Bryant et al. v. Compass Group U.S.A. Inc.* The court held that the defendant company's failure to provide the plaintiff with informed consent to the collection of her biometric data caused the plaintiff to suffer a concrete injury under the BIPA. This is a seminal case because it permits standing for a violation of a procedural right that did not result in any tangible injury to the claimant.

Saikali: There have been a series of recent federal cases that appeal to loosen the standing requirements for plaintiffs who allege harm following a data breach or privacy violation. Whether it is the Seventh Circuit's decision in *Remijas v. Neiman Marcus* or the Northern District of California's decision in the *Adobe* case, courts appear more open to allowing privacy cases to move forward based on a mere risk of harm.

CD: What hurdles do claimants and funders need to overcome to get a data protection class action off the ground?

Hadwin: *Lloyd v Google* was brought on a representative action basis and although this opt-out mechanism is not novel to the English courts, it has not traditionally been used in the context of large-scale data breaches. The outcome of the judgment will therefore help to establish a precedent for whether this opt-out route can be pursued in future or the more restricted GLO 'opt-in' mechanism,

will be the only viable option for taking mass action. Claimants might also struggle on evidential hurdles. Where claimants are seeking compensation for distress, assumptions are being applied by claimants that being affected by a data breach will naturally cause distress on the part of affected individuals. Defendants are taking an evidential approach to this issue – while genuine distress caused by a breach of a controller's GDPR obligations is compensable, evidence should be provided of this and no assumptions should be made, particularly in circumstances where the affected data set and the broader factual matrix are of limited sensitivity.

Collins: Historically, standing was a key hurdle because it traditionally required a showing of a concrete and particularised injury, such as suffering identity theft after a data breach. However, in recent years, courts have begun relaxing the standard for standing in data protection cases. Several key courts have allowed claims to go forward in data breach cases based on a finding that plaintiffs suffered an increased risk of identity theft. This trend is occurring outside of data breach cases as well. For instance, the Ninth Circuit Court of Appeals recently permitted plaintiffs' claims against a social media company to go forward after finding that mere violation of privacy constituted a concrete injury for standing purposes. Similarly, courts enforcing BIPA have recently found that plaintiffs do not need to prove an injury separate and apart from the statutory violation. This provides standing for claims relating to inadequate disclosures about the collection of biometric information even where no actual mishandling of data occurred.

Saikali: The biggest hurdles are demonstrating legally cognisable harm and causation. Both are challenging in data breach class actions because plaintiffs rarely suffer unreimbursed financially quantifiable harm, and it is unusual in many of these lawsuits, particularly the new ones focusing on ransomware attacks, that personal information was exfiltrated as part of the attack. On top of that, it is almost impossible to determine who or what was the cause of any identity theft or alleged fraudulent charges.

Henderson: For claims brought under an opt-in mechanism, and assuming that the merits of the claim are sufficiently strong, the primary challenge for claimant law firms and litigation funders is to build a class that is sufficiently large that the claim is commercially viable – they need to build

sufficient 'critical mass'. They advertise these claims using 'no-win/no-fee' funding packages and using adverse costs cover insurance policies that reduce the risk of class members being ordered to pay the defendant's legal costs if the claim fails. The biggest challenge in building a sufficiently large book is human inertia – even when faced with an apparently risk-free opportunity to potentially make a recovery, many people will not join a claim, even more so if the individualised losses are not significant or if the defendant's behaviour is not seen as being particularly egregious.

CD: What are the main challenges and issues facing litigators on both sides during a data protection class action?

Henderson: Aside from merits and quantum, the claimant law firm will face a number of logistical challenges, such as communicating with the class members, in which they will be helped by specialist vendors, and managing witnesses and evidence. There is often also informational asymmetry between the claimant class and the defendant, which the claimants will hope to equalise through disclosure or discovery. On the defendant side, these are high stakes and higher-pressure disputes with reports potentially going to the general counsel and the board. The narrative may be highly contentious and traumatic for senior executives and the defendant. The defendant and its lawyers may also need to address reputational and regulatory issues and possibly also defend parallel group proceedings filed in multiple jurisdictions, all of which requires careful coordination.

Saikali: For defence counsel, a challenge is educating the factfinder about the underlying technology in a way that makes it easy to understand, so the factfinder realises that the nature of the plaintiff's allegations are technically impossible or incredibly unlikely.

Collins: Defending data breach cases has become increasingly difficult as courts relax the standard for standing to sue and more cases survive past the motion to dismiss stage into discovery. At that point, defendants face the added challenge of protecting data breach reports from discovery. Courts have created a relatively high bar for successfully asserting privilege over such reports, and plaintiffs often fight aggressively for them because they may contain a road map of the deficiencies and issues that may have led to the breach.

Hadwin: Significant data breaches often lead to a number of different claimant law firms seeking to invite affected data subjects to join 'their' action. Given that there is no ready way of establishing which claimant law firm will be established as the 'lead' claimant firm, it is not uncommon to have a number of actions being issued by multiple firms

across multiple jurisdictions. These claims will inevitably not be presented in exactly the same way and time frames may differ, which presents challenges for defendant law firms that must, based on the same set of facts, subsequently defend these claims in a number of different ways under varying time constraints. Data breaches that only affect a limited number of data subjects pose different challenges. The per-claimant value of claims in this area tends to be low unless financial loss is alleged, the high-water mark of £12,500 in *TLT and others v The Secretary of State for the Home Department and the Home Office* being something of an outlier in this regard. Given costs for both bringing and defending a claim of this nature can far exceed the potential damages award, it can be difficult to justify action in these circumstances in a way which makes economic sense.

CD: How would you characterise the attitude of courts to data protection class actions in your jurisdiction?

Saikali: You cannot generalise the attitude of courts. Some courts have lower bars to standing than others. I do think that when you take a 30,000-foot view, you see that courts are more open to privacy and data security class actions now than they were five or 10 years ago.

Collins: As data breaches become more common and data privacy is an increasing public concern, federal and state courts seem to be open to new concepts of injury. This has eased the burden of bringing class action lawsuits against companies victimised by data breaches. This trend, however, is also seemingly consistent with legislative intent as more states adopt data protection legislation or expand the coverage of existing laws.

> **"Defending data breach cases has become increasingly difficult as courts relax the standard for standing to sue and more cases survive past the motion to dismiss stage into discovery."**
>
> *Alexis Collins, Cleary Gottlieb*

Hadwin: Navigating largely unchartered waters, the attitude of English courts appears to be mostly uncertain at this point. Most case law has been relatively controller-friendly and has focused on the evidential burdens which claimants face in

this space. In contrast, looking to *Lloyd v Google*, the Court of Appeal's finding that loss of control of personal data can itself equate to compensable damage hints to a more consumer-friendly approach. The outcome of the Supreme Court appeal in that case will therefore be crucial. Further, while the representative action procedure is longstanding it has only very recently been used to pursue 'mass' claims. Again, it seems English courts are still very much finding their way when it comes to applying the procedure in a proportionate and effective way.

Henderson: The English courts are well developed in their approach to data protection claims. The important decision of *Vidal-Hall v. Google* confirmed the entitlement to damages for distress back in 2014. Since then, we have had a regular stream of claims seeking damages for distress. In 2017, the High Court established the Media and Communications List which is intended to hear data protection claims, as well as more traditional media claims. This recognises both the need for these claims to be heard by specialist judges and that the volume of these claims justified its own list in the High Court. In October 2019, the English procedural rules introduced a specific pre-action protocol for media and communication claims which encompasses data protection actions. The introduction of this protocol again indicates the increasing volume of data protection claims.

"I think it is likely that we will keep seeing an uptick in 'big ticket' litigation in the months and years ahead because I see no slowing down of the statutory private rights of action."

Al Saikali,
Shook, Hardy & Bacon L.L.P.

CD: Looking ahead, do you expect the regulatory landscape to provide fertile ground for data protection class actions? How likely is that we will see a significant uptick in 'big ticket' litigation in the months and years ahead?

Hadwin: The outcome of the Supreme Court *Lloyd v Google* judgment will certainly go some way in determining how fertile the future ground will be for data protection class actions. A Supreme Court finding which echoes the decision of the Court of Appeal will no doubt spur claimant law firms across the UK. That said, the facts of *Lloyd v Google* cannot be universally applied to all data breaches. With

other class action decisions on the horizon, there are certainly a number of novel and contested issues which will continue to develop in the coming months and years – what seems clear, however, is that increased litigation in this area is here to stay.

Henderson: Although there are a number of important unanswered questions, the key issue is whether a workable procedure for bringing opt-out data protection class actions will become properly established. The Supreme Court's response to the appeal in *Lloyd v. Google* will address this issue. However, and distinct from that appeal, the UK government is presently consulting on introducing an amendment to the Data Protection Act that would permit non-profit organisations to bring claims for data protection breaches without the authority of the affected persons, likely on an opt-out basis. There will be a report to parliament on 25 November 2020. This process could lead to a new statutory mechanism for bringing collective data protection claims. If a workable procedure is established by either of the above routes, then further very high value data protection class actions are likely to be filed in the coming months and years.

Collins: We do expect it will be fertile ground, particularly if there is no federal privacy legislation. Class action plaintiffs typically bring data protection cases under state negligence or consumer protection laws. The patchwork of disparate legal and regulatory standards that is emerging through these cases in turn may make compliance by companies more difficult and increase the costs of litigation. Moreover, claims and settlement amounts are making headlines. For example, in 2020 Facebook agreed to pay $650m to users in one state to settle a class action over the company's use of facial recognition software. The uptick in settlement amounts will surely create the perfect storm for 'big ticket' litigation.

Saikali: I think it is likely that we will keep seeing an uptick in 'big ticket' litigation in the months and years ahead because I see no slowing down of the statutory private rights of action. The BIPA litigation in Illinois, for example, will likely cost companies millions, if not billons, of dollars adding up the total of damages and costs of defence. That is just one law. More have been recently implemented or are on the way in California, New York, Illinois, Massachusetts and elsewhere. CD