Data breach litigation and regulatory enforcement: A survey of our present and how to prepare for the future

Received (in revised form): 27th November, 2017

Behnam Dayanim
is a partner in the Washington, DC office of the international law firm Paul Hastings LLP, where he is global co-chair of the Privacy and Cybersecurity Practice and chair of the Advertising and Gaming Practice.

Paul Hastings LLP, 875 15th Street, N.W., Washington, DC 20005, USA
Tel: +1 202 551 1737; E-mail: Bdayanim@Paulhastings.com

Edward George
is an associate in the Privacy and Cybersecurity Practice and the Advertising and Gaming Practice groups.

Paul Hastings LLP, 875 15th Street, N.W., Washington, DC 20005, USA
Tel: +1 202 551 1922;, E-mail: edwardgeorge@Paulhastings.com

Abstract Americans have grown accustomed to the drumbeat of data breaches, particularly because most have involved credit card data where individuals are protected from harm and almost never suffer out-of-pocket losses. But the more recent data breaches — Equifax, Yahoo! and the United States Office of Personnel Management — raise new concerns because of the amount of highly sensitive data that has been compromised. These compromises have caught the attention of the Federal Trade Commission (FTC), state attorneys general and Congress, and, as a result, the approaches to privacy-related harms are changing. This paper explores the circuit courts of appeals' approaches to privacy harms in data breach cases, specifically with regard to Article III standing, and the FTC's approach in its privacy and cyber security enforcement actions. After examining both approaches, this paper concludes with insights into best practices on dealing with the shifting legislative, judicial and regulatory climate surrounding breaches.

KEYWORDS: privacy, cyber security, data breach, standing, Federal Trade Commission, circuit courts of appeals, emerging trends

INTRODUCTION

In September 2017, Yilum Wang and Michal Kosinski released the results of a study suggesting that facial recognition software can correctly identify an individual's sexuality.[1] 'The researchers culled tens of thousands of photos from an online-dating site, then used an off-the-shelf computer model to extract users' facial characteristics.'[2] The data was then fed into their own model,

which classified users by their supposed sexuality with unnerving accuracy. For men, the model was right 81 per cent of the time, and 71 per cent of the time for women. Humans, on the other hand, only picked correctly 61 per cent for men and 54 per cent for women.[3]

The study immediately drew fire from the Human Rights Campaign and GLAAD, two leading LGBTQ groups, for 'wrongfully suggesting that artificial intelligence (AI) can be used to detect sexual orientation'.[4] The groups offered a list of complaints, which the researchers rebutted point by point. But while the debate over the research still rages, Wang and Kosinski's point stands: companies and governments are increasingly using computer vision algorithms to detect people's intimate traits.[5] Indeed, this study is but one example of algorithms making decisions based on physical traits.[6] Take, for example, the collection and use of voice data. The human voice can be data mined to detect gender, race, age and even emotion.[7]

None of this is particularly surprising. For years companies have been collecting personal data through both the Internet and our smart devices in order to target advertising to desired demographics or even to match individuals' behaviour or preferences.[8] And while most consumers are OK with this type of targeting,[9] it does not diminish the fact that, somewhere, there is a bot or algorithm pouring over our data points, grasping for ways to connect any two of them. And therein lies the worry.

The Equifax breach in September 2017 reportedly exposed the personal data of over 143m Americans — approximately 44 per cent of the population. The compromised data included social security numbers, full names and birth dates.[10] Following Equifax's breach was the revelation that Yahoo's 2013 e-mail hack actually compromised all 3bn Yahoo accounts, revealing names, birth dates, phone numbers and passwords.[11] Even more disturbing, perhaps, was the 2015 Office of Personal and Management (OPM) breach, in which hackers gained access to the federal government's SF-86 forms, 'documents used for conducting background checks for worker security clearances', which contain 'a wealth of sensitive data not only about the workers seeking clearance, but also about their friends, spouses and other family members'.[12]

Equifax, Yahoo and OPM are not anomalies; hacks involving a host of prominent retailers and other companies have made headlines.[13] The consequence of these hacks is that there are now troves of data floating around black markets, allowing anyone with decent technical skills to uncover some of our most intimate secrets. And as we are seeing these data breaches continue to populate news headlines, we are seeing courts and the FTC treat data privacy-harms in a different light, raising the stakes and potential liability for companies.

Americans have grown accustomed to the drumbeat of breaches, particularly because most have involved credit card data where individuals are protected from substantial harm and almost never suffer out-of-pocket losses. However, the more recent breaches — Equifax, Yahoo and OPM — have raised concerns in a new and different way, particularly the amount of highly sensitive data that has been compromised. The FTC, state attorneys general and Congress have taken note, publicly announcing investigations, holding hearings and calling for stiffer consequences for companies that fail to take adequate steps to protect personal data.

This paper examines the emerging approaches to privacy-related harms that stem from data breaches. The first section discusses the circuit courts of appeals' approaches to privacy harms in data breach cases, specifically the circuit split regarding the issue of Article III standing. The second section discusses the FTC's approach in its own privacy and security enforcement actions. Lastly, the third section offers some insight into emerging trends and best

practices on how to deal with the shifting legislative, judicial and regulatory climate on these issues.

JUDICIAL APPROACHES TO PRIVACY HARMS

The most hotly contested issue in data breach lawsuits to date has been the question of harm. When plaintiffs bring suit in federal court, they will have to demonstrate that they suffered harm sufficient to establish Article III standing. The Supreme Court, in 1992, set forth the requirements of the constitutional standing doctrine in *Lujan v. Defenders of Wildlife.*[14] To possess Article III standing, a plaintiff must have, among other things, suffered an injury-of-fact.[15] Yet, since *Lujan*, the circuit courts have been divided over what constitutes an 'injury of fact', specifically with respect to 'future harm'.

The Supreme Court has tried to clarify the scope and contours of standing in data privacy contexts twice in the past five years — first in *Clapper v. Amnesty International*[16] and then in *Spokeo Inc. v. Robbins*.[17] In *Clapper*, the court held that for plaintiffs to possess standing for a future harm, the injury must be 'concrete, particularized, and actual or imminent'; the mere anticipation of non-imminent harm is insufficient.[18] After *Clapper*, a majority of courts ruled that 'injuries from data breaches are too speculative and hypothetical' to warrant standing.[19] In *Spokeo*, the court 'tried to clarify the harm required for standing when injuries resulted from the mishandling of personal data'.[20] The court held that harm required for standing must be concrete, 'yet it suggested that "intangible harm", and even the "risk" of harm, could be sufficient to establish harm if intangible injury has a "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts"'.[21]

Despite the court's attempts in *Clapper* and *Spokeo* to clarify standing for 'future harm', the issue remains muddled, with nine of the 12 geographic federal courts of appeals adopting contrasting approaches in the context of data breaches.[22]

One preliminary note: these cases, and the ensuing discussion, focus exclusively on consumer harms. One category of plaintiffs that has demonstrated little trouble in establishing standing in data breach litigations is financial institutions.[23] Financial institution plaintiffs have successfully brought suit and extracted substantial settlements in cases arising from breaches of credit and debit card information.[24] The reason for this success is simple: card-issuing banks always suffer losses from card breaches. Those losses include costs of fraudulent transactions and the issuance of new cards to replace those that have been compromised.

Yet, not every breach is a card breach, and the far greater potential liabilities lie with consumer claims. Hence, that is the focus of this discussion.

Circuits finding that future harm may provide standing

Four circuit courts of appeals have found allegations of future harm in at least one instance sufficed to confer standing on plaintiffs.

Sixth Circuit: *Galaria v. Nationwide Mut. Ins. Co.*[25]

In *Galaria*, the plaintiffs sued Nationwide Mutual Insurance because hackers had breached its computer network and stole plaintiffs' personal information.[26] Among the plaintiffs' claims, they argued that Nationwide 'willfully and negligently' violated the Fair Credit Reporting Act (FCRA) by 'failing to adopt required procedures to protect against wrongful dissemination of plaintiffs' data'.[27] To support their claims, plaintiffs also argued that Nationwide's data breach 'created an "imminent, immediate and continuing increased risk"' that they would be subject

to identity fraud because 'there is an illicit international market for stolen data, which is used to obtain identification, government benefits, employment … and credit and debit cards'.[28] Further, the plaintiffs argued that 'victims of identity theft and fraud will "typically spend hundreds of hours in personal time and hundreds of dollars in personal funds"'.[29]

The district court dismissed the complaint, concluding that plaintiffs lacked Article III standing, among other things.[30] However, the Sixth Circuit thought differently. The court first cited *Spokeo* for the proposition that '[t]o establish injury in fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical"'.[31] The court then found the 'allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs', sufficient to establish Article III injury.[32] Notably, the court pointed to Nationwide's decision to provide a year's credit monitoring and identity theft protection to victims of the data breach — a routine measure in breach cases — as support for its ruling, characterising the company's decision as implicit recognition of the possibility of future injury.[33] The court added: '[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for fraudulent purposes.'[34]

Seventh Circuit: *Remijas v. Neiman Marcus Grp., LLC*[35]

In 2013, hackers attacked Neiman Marcus, stealing the credit card numbers of 350,000 customers.[36] Neiman Marcus eventually notified its customers who were affected, 'offering them one year of free credit monitoring and identity-theft protection'.[37] Following Neiman Marcus' announcement of the breach, plaintiffs filed a class action, relying on a number of theories for relief including 'negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws'.[38] Neiman Marcus moved to dismiss the complaint, citing lack of standing and for failure to state a claim. The district judge exclusively granted the motion on a purported lack of standing by plaintiffs.[39]

The Seventh Circuit reversed, stating that '[a]llegations of future harm can establish Article III standing if that harm is "certainly impending", but "allegations of possible future injury are not sufficient"'.[40] Because 9,200 people had already incurred fraudulent charges, the court held that those people 'have suffered the aggravation and loss of value of the time needed to set things straight', which is sufficient for standing.[41]

More strikingly, the court further determined that the remaining 340,800 customers who had not yet suffered fraudulent charges also possessed standing because they 'should not have to wait until hackers commit identity theft or credit card fraud in order to … [have] standing'.[42] 'Requiring the plaintiffs "to wait for the threatened harm to materialize in order to sue" would create a different problem: the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach.'[43] While *Remijas* predates *Spokeo*, it appears to remain controlling within the Seventh Circuit, with numerous cases citing or invoking it since the Supreme Court decision.[44]

Ninth Circuit: *Krottner v. Starbucks Corp.*[45]

The Ninth Circuit was the first appellate court to find Article III standing based solely on future harm in the context of a data breach. In 2008, a laptop was stolen from Starbucks that contained the 'unencrypted names, addresses and social

security numbers of approximately 97,000 Starbucks employees'.[46] Starbucks alerted its employees to the theft and provided a free credit monitoring service for one year.[47] Three plaintiffs separately sued Starbucks, alleging that Starbucks acted negligently and breached an implied contract under Washington law.[48]

The district court dismissed the case, holding that while plaintiffs had standing under Article III, they did not 'allege a cognizable injury under Washington law'.[49] The question presented to the Ninth Circuit was whether the plaintiffs adequately had alleged an injury-of-fact.[50] The court found that one of the plaintiffs sufficiently alleged a present injury that was sufficient to confer standing — heightened 'anxiety and stress' as a result of the breach — before turning to the question of 'whether an increased risk of identity theft constitutes an injury-in-fact'.[51]

The court stated that if 'a plaintiff faces "a credible threat of harm", and that harm is "both real and immediate"', then the plaintiff will meet the injury-in-fact requirement.[52] The court determined that the Starbucks employee plaintiffs had a 'credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data'.[53] Because the laptop had actually been stolen, the court found that the plaintiffs' allegations were not merely conjectural or hypothetical. In the court's view, the risk of identity theft or credit card fraud was credible, real and immediate.[54] *Krottner* also pre-dates *Spokeo* but since has been cited by numerous cases in the context of discussions of standing.[55]

DC Circuit Court of Appeals: *Attias v. CareFirst, Inc.*[56]

Attias v. CareFirst, Inc. dealt with CareFirst, a health insurer that suffered a cyberattack in 2014 resulting in unauthorised access and possible theft of its policyholder customers' information.[57] After the company announced the breach, seven customers brought a putative class action, raising 'eleven different state-law causes of action, including breach of contract, negligence, and violation of various state consumer-protection statutes'.[58] The plaintiffs tried to certify a class of all CareFirst customers living in Maryland, Virginia and DC whose information had been compromised. CareFirst moved to dismiss for a lack of Article III standing, and the district court agreed, finding that the plaintiffs neither presented a 'present injury nor a high enough likelihood of future injury'.[59] The district court believed that the plaintiffs' argument that they suffered an increased risk of identity theft because of the breach was too speculative a theory of injury.[60]

The DC Circuit disagreed. The court observed that, as set out in *Spokeo*, '[a]n injury in fact must be concrete, particularized, and, most importantly for our purposes, "actual or imminent" rather than speculative'.[61] It must also be 'fairly traceable to the challenged conduct of the defendant'.[62] The court found that the risk that the hackers accessed plaintiffs' social security or credit card numbers and the fact that the 'combination of members' names, birth dates, email addresses and subscriber identification numbers' can qualify as personal information, coupled with the very real possibility of 'medical identity theft', sufficed for a plausible allegation that the plaintiffs faced a substantial risk of identity fraud.[63] Further, the court found that it is not speculative to assume that the hackers have both the 'intent and ability to use [the stolen] data for ill'.[64] '[S]imply by virtue of the hack and the nature of the data' that was taken, the court determined that a substantial risk of harm already existed.[65]

Circuits finding allegations of future harm insufficient

Five circuit courts of appeals have rejected arguments of standing predicated on potential future harm.

First Circuit: *Katz v. Pershing, LLC*[66]

In *Katz*, the defendant sold 'brokerage execution, clearance, and investment products and services to other financial organizations'.[67] One service offered by the defendant was an electronic platform that allowed end-users to access remotely 'a wealth of information about market dynamics and customer accounts'.[68] The plaintiff argued that the defendant failed to 'protect sensitive nonpublic information as it was obligated to do under both contract and consumer protection laws'.[69] Specifically, the plaintiff was concerned that 'her nonpublic personal information ha[d] been left vulnerable to prying eyes because it [wa]s inadequately protected by the defendant's service'.[70]

As is the pattern in these cases, the district court dismissed for lack of Article III standing. However, this time, unlike in the other circuits discussed above, on appeal, the First Circuit upheld the district court. The court stated that because the plaintiff alleged 'only that there is an increased risk that someone might access her data', and did 'not identify any incident in which her data has ever been accessed by an unauthorized person, she cannot satisfy Article III's requirement of actual or impending injury'.[71] *Katz* pre-dates *Spokeo*, but it remains controlling law in the First Circuit, having been cited by over a dozen cases addressing standing since the *Spokeo* decision, with no case in that circuit appearing to repudiate it.

Second Circuit: *Whalen v. Michaels Stores, Inc.*[72]

In *Whalen*, the plaintiff, in 2013, made a purchase on her credit card at a Michaels store (part of the national crafts retail chain) on 31st December.[73] Following her purchase, the plaintiff alleged in her complaint that on 14th January, 2014, her credit card was physically presented 'for payment to a gym in Ecuador', and on 15th January, her credit card was also physically presented in Ecuador to purchase a concert ticket.[74] The plaintiff cancelled her credit card on 15th January, and shortly thereafter Michaels confirmed a data breach involving the theft of customers' credit and debit card information.[75] The plaintiff then sued, asserting claims for breach of contract and other causes of action, but the district court held that the allegations in the complaint were insufficient because the plaintiff 'neither alleged that she incurred any actual charges on her credit card, nor, with any specificity, that she had spent time or money monitoring her credit card'.[76]

The Second Circuit, in a summary order, affirmed the dismissal, 'concluding that [the plaintiff] had failed to allege a cognizable injury from the exposure of her credit card information following a data breach at one of Michaels' stores'.[77] The court noted that the plaintiff did 'not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly cancelled after the breach and no other personally identifiable information — such as her birth date or Social Security number — is alleged to be stolen'.[78] The *Whalen* decision was issued after *Spokeo*, although the court does not cite or otherwise invoke the Supreme Court precedent in its analysis.

Third Circuit: *Reilly v. Ceridian Corp.*[79]

Ceridian, a payroll processing firm, collects information about its customers' employees, including names, addresses and social security numbers, in order to process its customers' payrolls.[80] Ceridian suffered a security breach in 2009, allowing unauthorised access to personal and financial information belonging to 27,000 employees at 1,900 companies.[81] The court stated without elaboration that it was never known whether the 'hacker read, copied, or understood the data'.[82] (The court does not indicate whether the data were in some format or medium that was particularly difficult to read or understand; presumably, the data were not encrypted as that may have provided a basis on which to decide

not to notify customers of the incident.) Ceridian sent letters to the potential identify theft victims, informing them of the breach, and — again, as is the usual practice — provided one year of free credit monitoring and identity theft protection.[83] The plaintiffs sued Ceridian, alleging that they faced an increased risk of identity left, incurred costs to monitor their credit activity and suffered from emotional distress as a result of the breach.[84]

The Third Circuit upheld the district court's dismissal of the suit, stating that 'allegations of hypothetical, future injury' are not sufficient to satisfy Article III.[85] The court noted that the mere fact that the hacker may have read, copied and understood the personal information, intends to commit future crimes with that information, and is able to use that information to the plaintiffs' detriment is far too speculative to achieve injury of fact.[86] *Reilly*, like the First Circuit's decision in *Katz*, was issued before the Supreme Court's decision in *Spokeo*, but courts in the Third Circuit continue to rely on it as authoritative in analysing challenges to standing, and we are aware of no decision in the Third Circuit since *Spokeo* declining to follow *Reilly* on that basis.

Fourth Circuit: *Beck v. McDonald*[87]

In *Beck*, the William Jennings Bryan Dorn Veterans Affairs Medical Center (Dorn VAMC) in Columbia, South Carolina, suffered two data breaches — one in 2013, in which a laptop containing the personal information of about 7,400 patients was stolen, and a second in 2014, in which four boxes of pathology reports containing information on 2,000 individuals went missing.[88] Patients brought separate putative class actions, one for the 2013 breach ('Beck') and a second for the 2014 breach ('Watson'), against the Secretary of Veteran Affairs and Dorn VAMC, alleging violations of the Privacy Act of 1974 and other claims.[89] In both actions, the plaintiffs tried to establish Article III standing by arguing that there is 'harm from the increased risk of future identity theft and the cost of measures to protect against it'.[90] The district court dismissed the actions because the plaintiffs 'failed to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing'.[91]

The plaintiffs appealed, the cases were consolidated, and the Fourth Circuit upheld the district court. The court distinguished this case from the situations in *Galaria* and *Remija*. In the court's view, the Beck plaintiffs, unlike in *Galaria* and *Remija*, 'uncovered no evidence that the information contained on the stolen laptop ha[d] been accessed or misused or that they … suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to seal their private information'.[92] The court further stated that the Watson plaintiffs' complaint suffers 'from the same deficiency with regard to the four missing boxes of pathology reports'.[93] Moreover, the court noted, that '"as the breaches fade further into the past", the Plaintiffs' threatened injuries become more and more speculative'.[94]

Eighth Circuit: *In Re: SuperValu, Inc.*[95]

Similar to *Remijas*, hackers twice attacked SuperValu, a retail grocery store, stealing its customers' financial information, including 'their names, credit or debit card account numbers, expiration dates, card verification value codes, and personal identification numbers'.[96] The plaintiffs sued, contending that the breaches subjected them 'to an imminent and real possibility of identity theft', specifically that the hackers could use their information to 'siphon money from their accounts'.[97]

As in the previous cases, SuperValu moved to dismiss the complaint, arguing the plaintiffs had no standing because there was no injury of fact.[98] The district court granted the motion, concluding that

'because the complaint alleged only an "isolated single instance of an unauthorized charge"', there was 'insufficient evidence of misuse of plaintiffs' [information] connected to [SuperValu's] data breach to "plausibly suggest that the hackers had succeeded in stealing the data and were willing and able to use it for future theft or fraud"'.[99]

The Eighth Circuit, invoking *Spokeo*, found that while the plaintiffs sufficiently alleged 'that their [information] was stolen by hackers as a result of [SuperValu's] security practices', they did not succeed in showing that the information was misused.[100] The court noted that the allegedly stolen information did not include 'any personally identifiable information, such as social security numbers, birth dates, or driver's license numbers' and therefore, given the factual information asserted in the complaint, 'there is little to no risk that anyone will use the [information] to open unauthorized accounts in the plaintiffs' names'.[101] Thus, the court found that the complaint did not sufficiently allege a substantial risk of identity theft, and, as a result, the plaintiffs' allegations of future injury did not support standing.[102]

SO WHERE DO WE STAND?

The issue of whether future harm is sufficient to confer standing remains muddled in the post-*Spokeo* world. Standing in many cases seems to turn on how artfully pled is the complaint. At the same time, some courts seem more sceptical of arguments of future harm than do others, while some — the Sixth Circuit in *Galaria* offers one example — impute great significance into measures, such as offering consumers free credit monitoring, that have become staples of almost any incident response, even where there is believed to be little risk of harm.

That said, it does seem as if courts increasingly will be confronting new and substantial arguments of harm — arguments that often will suffice to confer standing. As breaches move beyond card data to include far more sensitive indicia of personal information, those arguments will become even more compelling. As standing objections start to fall by the wayside, judicial scrutiny increasingly will turn to questions of fault and responsibility — what did the defendant do to protect the data from breach?

In examining those issues and thinking about how best to protect oneself from liability, a review of federal regulatory enforcement in this area is instructive.

THE FEDERAL TRADE COMMISSION'S APPROACH TO PRIVACY HARMS RESULTING FROM DATA BREACHES

Courts have not been alone in considering the implications of data breaches on privacy harms. Federal agencies, such as the Federal Communications Commission, Consumer Financial Protection Bureau and Office of Civil Rights of the Department of Health and Human Services (OCR), as well as state attorneys general, also have become actively involved. Agencies are not fettered by considerations of standing that often have resulted in termination of judicial actions well before any examination of underlying culpability. For that reason, agency enforcement trends offer the clearest window to date into how corporate culpability is determined.

Undoubtedly the most prominent actor in establishing regulatory expectations through early and aggressive enforcement and industry guidance has been the FTC. (OCR also has been extremely active, although confined to the healthcare sector, where very specific regulatory requirements often dictate liability.) Since 2002, the FTC has brought over 60 cases against companies that in the agency's view put consumers' personal data at unreasonable risk.[103] The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act.[104] Section 5 prohibits unfair or deceptive practices in or that affect interstate commerce.[105]

Deception cases are straightforward: if you promise to undertake or to refrain from undertaking a specific activity or practice, and then you violate that promise, causing actual or probable harm, that is 'deceptive'. For example, in 2016, a Singapore-based mobile advertising company paid US$950,000 in civil penalties for allegedly deceptively tracking the location of millions of customers, despite telling the customers it would only track them if they opted in.[106]

The more novel issue presented by recent FTC actions — and the one most relevant to understanding the extent of potential liability in the event of breach — is the agency's understanding of what is 'unfair' in the data security context. This section outlines three FTC enforcement actions that shed light on that question.

FTC v. Wyndham

Wyndham Worldwide, a hospitality company that franchises and manages hotels, suffered three separate successful attacks on its information systems in 2008 and 2009.[107] In April 2008, hackers broke into the network of a hotel in Phoenix, Arizona, which granted them access to Wyndham's network.[108] Once inside the network, the hackers used a brute-force method — repeatedly guessing users' login IDs and passwords — to access an administrator account, and that access allowed them to obtain unencrypted information for over 500,000 accounts.[109] In March 2009, hackers attacked again, accessing Wyndham's network through an administrative account, resulting in complaints from customers about fraudulent charges.[110] In this attack, hackers 'obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels'.[111] Finally, in late 2009, hackers breached the network once again by accessing an administrator account on one of its networks.[112] Here, the hackers obtained credit card information for approximately 69,000 customers from the property management systems of 28 hotels.[113]

The FTC alleged that, in total, the hackers accessed over 619,000 consumers' information, resulting in at least $10.6m in fraud loss.[114] The FTC stated that 'consumers suffered financial injury through "unreimbursed fraudulent charges, increased costs, and lost access to funds or credit", and that they "expended time and money resolving fraudulent charges mitigating subsequent harm"'.[115] In 2012, the FTC filed suit, claiming that Wyndham had engaged in 'unfair' and 'deceptive' practices in violation of Section 5(a). Wyndham filed a Rule 12(b)(6) motion to dismiss both claims, and the district court 'denied the motion but certified its decision on the unfairness claim for interlocutory appeal', which the Third Circuit granted.[116]At issue before the Third Circuit was whether the FTC had 'authority to regulate cyber security under the unfairness prong of § [5(a)]; and, if so, whether Wyndham had fair notice its specific cyber security practices could fall short of that provision'.[117]

Wyndham argued that its practices did not fall within the plain meaning of 'unfair' because they were not '[in]equitable' or 'marked by deception'.[118] The court disagreed, observing that a company does not act 'equitabl[y] when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cyber security, exposes its unsuspecting customers to substantial financial injury, and retains the profits to their business'.[119]

Wyndham also asserted that a business cannot be found to have treated its victims unfairly when the company itself was the victim of a criminal act which led to the alleged unfairness. The court also rejected that contention, affirming the FTC's ability to bring claims based on likely injury to consumers, even if the business was also a victim.[120]

Notably, Wyndham also maintained that Congress impliedly excluded data security from the FTC's general 'Section 5' jurisdiction by passing separate sector-specific data security legislation.[121] Wyndham argued that the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act and the Children's Online Privacy Protection Act granted the FTC authority to regulate data security only within limited areas and that such grants of authority would have been superfluous if the FTC could have regulated data security under Section 5.[122] The court disagreed and instead found that the acts simply expanded the FTC's powers beyond those contained in Section 5.[123]

Lastly, Wyndham argued that it lacked fair notice regarding the data security standards it was required to meet.[124] The court rejected that contention, stating that '[f]air notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of [a] statute'.[125]

Here, the agency had accused Wyndham of failings in several specific areas:

- Allowing its franchised hotels to 'store payment card information in clear readable text';[126]
- Allowing the use of 'easily guessed passwords to access the property management systems';
- Failing to use '"readily available security measures" — such as firewalls — to "limit access between [the] hotels' property management systems, … corporate network, and the Internet"';
- Allowing 'hotel property management systems to connect to its network without taking appropriate cyber security precautions', including ensuring the use of updated operating systems, preventing the use of default user IDs and passwords and maintaining an accurate inventory of computers connected to the Wyndham network;
- Failing to limit third-party-vendor access to its systems to the minimum necessary;
- Failing to 'employ "reasonable measures to detect and prevent unauthorised access" to its computer network or to "conduct security investigations"'; and
- Failing to follow 'proper incident response procedures'.[127]

Wyndham's alleged failure adequately to address these issues after the first breach, leading — in the agency's view — to two further breaches in rapid succession, almost certainly exacerbated Wyndham's exposure and hardened the agency's enforcement posture toward the company.

Wyndham is significant precedent because it marked the first time the FTC's authority to regulate data security under the unfairness prong of Section 5(a) was addressed and affirmed by a court. However, perhaps its greater significance lies in the agency's enumeration of what it found to be deficient in Wyndham's security measures.

The agency's message to companies holding personal data seems rather clear: certain steps (complex passwords, vendor management, systems inventory, incident response protocols) are always expected, and, once a company becomes aware its network is vulnerable, it is imperative it takes steps to redress those vulnerabilities promptly and effectively.

In the Matter of LabMD, Inc.

Perhaps the most colourful case addressing the FTC's authority to regulate 'unfairness' in the data security context involves a small Georgia-based clinical laboratory, LabMD. The case has spawned a slew of lawsuits, some of which still continue, as well as a self-published book bearing the provocative title *The Devil Inside the Beltway*, authored by the now-defunct company's CEO attacking the FTC, his former counsel and others.[128]

In 2008, Tiversa, a data security company, contacted LabMD, informing the lab that Tiversa had found a LabMD document containing personal information for

approximately 9,300 patients, including names, social security numbers, addresses and health insurance information on a peer-to-peer file sharing network.[129] Tiversa offered LabMD data security services, and after LabMD declined to pay, Tiversa reported LabMD to the FTC.[130]

Relying on information provided by Tiversa, the commission launched an investigation into LabMD's data practices in 2010, and in 2013 the FTC voted to issue a complaint.[131] Rather than enter into a consent agreement with the agency, agreeing to improve its security practices and likely paying a modest fine, LabMD contested the agency's determination that it was at fault. In 2013, the FTC filed an administrative complaint against LabMD, alleging that it had engaged in unfair data security practices.

After hearing the case, the administrative law judge ruled that the FTC needed to prov, under Section 5(n) that LabMD's 'practice causes or is likely to cause substantial injury to consumers'.[132] The judge found that the burden was on the agency to prove that the alleged failure to employ 'reasonable and appropriate' data security 'caused or is likely to cause, substantial injury to consumers'.[133] The judge held that the evidence presented failed to prove the allegations, and that, '[p]roof of a "risk" of harm, alone, "when divorced from any measure of the probability of occurrence, … cannot lead to useable rules of liability"'.[134]

The FTC appealed to the full commission. (Agency proceedings go first to an agency ALJ, followed by appeal to the full commission and only then to a federal appellate court.) The commission's opinion, written by Chairwoman Edith Ramirez, overturned the judge's decision, holding that the judge applied the wrong legal standard for unfairness.[135] The commission's resolution of this case turned in significant part on the meaning of the first prong of Section 5(n), which allows an act or practice to be deemed unfair if it 'causes or is likely to cause substantial injury to consumers'.[136] The commission held that 'a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low'.[137] After this holding, the commission applied Section 5(n)'s three-prong test to LabMD's security practices, finding it failed to provide reasonable security for the sensitive information on its servers and its failure was likely to cause substantial injury to its consumers.[138]

LabMD appealed the commission's decision to the Eleventh Circuit court of appeals, where, as of this writing, it remains pending.[139]

VIZIO, Inc.

VIZIO is distinct from *Wyndham* and *LabMD* in that it did not involve a 'data breach', nor did it rest solely on an 'unfair' lack of data security. Instead, it represents a significant expansion in the way in which the agency appears to view the sensitivity of what heretofore had been regarded (in the United States, at least) as relatively innocuous forms of personal data.

Between 2014 and 2016, VIZIO manufactured televisions that could continuously track what consumers were watching. The company also remotely installed the tracking software on previously sold televisions that, at time of sale, lacked that capability.[140]

Through the software, VIZIO's televisions transmitted consumers' viewing behaviour on a second-by-second basis. According to VIZIO, the software 'captured up to 100bn data points each day for more than 10 million VIZIO televisions', with the company allegedly storing this data indefinitely.[141] Further, while the data collected did not identify the viewers, the FTC alleged that VIZIO paired viewing data with other information about the television, including IP address, wire and wireless MAC addresses, WiFi signal strength and other items.[142]

VIZIO allegedly sold the data to third parties through licensing agreements for the purposes of analysing audience measurements, analysing advertising effectiveness and targeting advertising to 'particular consumers on their other digital devices based on their television viewing data'.[143] And VIZIO was allegedly doing all of this without explicitly telling consumers or getting their consent.[144]

When the FTC filed its complaint against VIZIO, it interpreted Section 5's unfairness prong in a novel way; specifically, the complaint alleged that VIZIO used the technology to 'comprehensively collect the sensitive television viewing activity of consumers or households' and deemed that tracking 'unfair'.[145] This was the first time the FTC labelled television viewing activity as sensitive information. The FTC alleged that the collection and sharing of this sensitive information without the consumers' consent had caused or is likely to cause substantial injury to the consumer.[146]

Ultimately, the case resulted in a Stipulated Order where VIZIO settled for US$2.2m, agreeing to delete all data collected up until March 2016 and to improve its privacy practices.[147]

EMERGING TRENDS AND BEST PRACTICES

Crystal balls are always perilous; however, in this case, some predictions are easy to venture. As data thieves find new and innovative ways to hack and monetise personal data, and as the types and extent of data collected continue to expand, courts increasingly seem likely to find sufficient harms to enable litigations to proceed.

That, in turn, will lead to increased focus on fault. Who — beyond the hacker — should be found liable for harm caused by a data breach? Theories of express or implied contract, negligence and the like will continue to come to the fore. Questions will include:

- What did you promise with respect to security?
- What measures did you have in place, and how do they compare to industry norms or regulatory requirements?

Sweeping statements that a company 'keeps its customer information secure' can expose that company to significant liability in the event of a compromise. Similarly, state or federal regulatory standards may be used to establish standards of care whose breach may be considered 'negligent', even if the regulatory frameworks themselves do not provide for private rights of action.

Beyond those obvious items, the agencies' own history of enforcement will provide a yardstick for plaintiffs against which to measure defendants' security measures. Weaknesses such as the use of default or easily guessed passwords, failure to use or properly to configure firewalls, poor vendor management and the like will invite findings of liability.

Key to all of these areas will be reasoned, deliberate decision making in establishing security policies and procedures. That, in turn, requires several key steps:

- Understand what information you are holding and where it is located. Until you know what you have and where it is kept, it is impossible to know what measures may be needed to protect it.
- Assess the information's legal and commercial sensitivity. Understand the statutory and regulatory requirements that attach to the information you hold, and also assess its business importance. It is impossible to protect all data equally well. Value judgments must be made, and differing levels of security ascribed based on both legal and business requirements. Both factors are critical. Reliance on either alone would be incomplete and create substantial potential exposure to loss.
- Manage your vendors. Know who they are and what they can access. Make deliberate

decisions in determining the extent and duration of that access, limiting it only to what is needed for them to perform their designated functions.
- Lastly, incident notification and remediation are critical. In the already notorious Equifax breach, part of the public opprobrium focused on Equifax's perceived ineptness in addressing the incident after it occurred — its failure to communicate internally to key stakeholders (possibly resulting in sales of shares by senior executives after the breach had occurred) and the length of time after the breach before the company began notifying consumers. Delays sometimes are inevitable, as companies attempt to figure out the scope and contours of a breach, but regulators are increasingly demanding prompt notifications. Already, for example, the New York Department of Financial Services requires notice to the agency within 72 hours of a breach,[148] and the new European General Data Protection Regulation imposes the same time frame.[149] As of this writing, Congress is considering national breach notification legislation, and several states are proposing to tighten their existing requirements.

Clear lines of authority and accurate understanding of systems and data are essential to timely and appropriate incident response. The only way to have confidence that a process will work is to test and test again. Companies that do not 'table-top' their incident response programmes risk unforeseen delays and inaccuracies when responding to a breach.

CONCLUSION

On the whole, it seems clear that companies can expect increasing demands to protect the data they possess — demands by regulators, legislators and courts. Regulators will continue to pursue cyber security cases where they perceive corporate negligence or inattention, and, in the courts, questions of standing increasingly will fall by the wayside, bringing the focus fully to bear on culpability and magnitude of harm. Companies that are not prepared can expect far greater consequences in the future than they have in the past.

Notes and References

1. Wang, Y. and Kosinski, M. (2017), 'Deep Neural Networks Are More Accurate Than Humans At Detecting Sexual Orientation From Facial Images', *Journal of Personality and Social Psychology*.
2. Alan Burdick (September 2017), *The A.I. "Gaydar" Study And The Real Dangers Of Big Data, New Yorker*, available at https://www.newyorker.com/news/daily-comment/the-ai-gaydar-study-and-the-real-dangers-of-big-data (accessed 24th January, 2018).
3. *Ibid.,* note 2.
4. *Ibid.,* note 2.
5. *Ibid.,* note 1.
6. Garvie, C., Bedoya, A. and Frankle, J. (October 2016), 'The Perpetual Line-Up Unregulated Police Face Recognition in America', Georgetown Law Center on Privacy & Technology, available at https://www.perpetuallineup.org/ (accessed 24th January, 2018).
7. Hughes, S. M. and Rhodes, B. C. (2011), 'Making Age Assessments Based on Voice: The Impact of the Reproductive Viability of the Speaker', *Journal of Social, Evolutionary and Cultural Psychology*, 4, p. 290, available at http://psycnet.apa.org/fulltext/2011-14971-007.pdf (accessed 24th January, 2018) (ability to identify gender, race, age); Smith, H. M. J., Dunn, A. K., Baguley, T. and Stacey, P. C. (February 2016), 'Concordant Cues in Faces and Voices: Testing the Backup Signal Hypothesis', *Evolutionary Psychology*, Sage Journals, available at http://journals.sagepub.com/doi/full/10.1177/1474704916630317 (accessed 24th January, 2018) (ability to identify emotions).
8. Hill, K. (February 2012), 'How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did', *Forbes*, available at https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#34af8c2e6668 (accessed 24th January, 2018).
9. Kirkpatrick, D. (May 2016), 'Study: 71% of consumers prefer personalized ads', Marketing Dive, available at https://www.marketingdive.com/news/study-71-of-consumers-prefer-personalized-ads/418831/ (accessed 24th January, 2018).
10. Newman, L. H. (September 2017), 'How to Protect Yourself From That Massive Equifax Breach', *Wired*,

available at https://www.wired.com/story/how-to-protect-yourself-from-that-massive-equifax-breach/ (accessed 24th January, 2018).
11. Perlroth, N. (October 2017), *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, *New York Times*, available at https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html (accessed 24th January, 2018).
12. 12 Zetter, K. and Greenberg, A. (June 2015), 'Why The OPM Breach Is Such A Security and Privacy Debacle', *Wired*, available at https://www.wired.com/2015/06/opm-breach-security-privacy-debacle/ (accessed 24th January, 2018).
13. 13 Harris, E. A., Perlroth, N. and Popper, N. (January 2014), 'Neiman Marcus Breach Worse Than First Said, *New York Times*, available at https://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html; Abrams, R. (May 2017), 'Target to Pay $18.5 Million to 47 States in Security Breach Settlement', *New York Times* https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html (accessed 24th January, 2018).
14. 504 U.S. 555 (1992).
15. *Ibid*. note 14.
16. 133 S. Ct. 1138 (2013).
17. 136 S. Ct. 1540 (2016).
18. *Clapper*, 133 S. Ct. 1147, 1155.
19. Solove, D. and Citron, D. (forthcoming), 'Risk and Anxiety: A Theory of Data Breach Harms', *Texas Law Review*, Vol. 96, No. 3.
20. *Ibid*., note 4.
21. *Ibid.,* note 4.
22. The Fifth, Tenth and Eleventh Circuits have not ruled on this issue.
23. *The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 1:14-md-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016) (holding that financial institutions have adequately pleaded standing by pleading actual injury in the form of costs to cancel and reissue cards compromised in the data breach).
24. Corso, J. (May 2017), 'Judge Approves $5.2M Kmart Breach Settlement With Caveat', Law360, available at https://www.law360.com/articles/926315/judge-approves-5-2m-kmart-breach-settlement-with-caveat (accessed 24th January, 2018).; Roberts, J. J. (March 2017), 'Home Depot to Pay Banks $25 Million in Data Breach Settlement', *Fortune*, available at http://fortune.com/2017/03/09/home-depot-data-breach-banks/ (accessed 24th January, 2018).; Stempel, J. and Bose, N. (December 2015), 'Target in $39.4 million settlement with banks over data breach', *Reuters*, available at https://www.reuters.com/article/us-target-breach-settlement/target-in-39-4-million-settlement-with-banks-over-data-breach-idUSKBN0TL20Y20151203 (accessed 24th January, 2018).
25. 663 Fed. Appx. 384 (6th Cir. 2016).
26. *Ibid*., note 26, 385.
27. *Ibid*., note 26 386.
28. *Ibid*., note 26.
29. *Ibid*., note 26.
30. *Ibid*., note 26, 385.
31. *Ibid*., note 26, 388 (quoting *Spokeo*, 136 S.Ct. at 1548).
32. *Ibid*., note 26.
33. *Ibid*., note 26.
34. *Ibid*., note 26.
35. 794 F. 3d 688 (7th Cir. 2015).
36. *Ibid*., note 35, 689.
37. *Ibid*., note 35, 691.
38. *Ibid*., note 35, 690–691.
39. *Ibid*., note 35, 691.
40. *Ibid*., note 35, 692 (emphases added).
41. *Ibid*., note 35,
42. *Ibid*., note 35, 693.
43. *Ibid*., note 35,
44. A comprehensive search of Westlaw did not yield any cases in the Seventh Circuit that appear to repudiate *Remijas.*
45. 628 F.3d 1139 (9th Cir. 2010).
46. *Ibid*., note 45, 1140–1141.
47. *Ibid*., note 45, 1141.
48. *Ibid*., note 45.
49. *Ibid*., note 45,
50. *Ibid*., note 451142.
51. *Ibid*., note 45.
52. *Ibid*. at 1143.
53. *Ibid*., note 45.
54. *Ibid*., note 45.
55. As with *Remijas*, *ibid*., note 44, comprehensive search of Westlaw did not yield any cases in the Ninth Circuit that appear to repudiate *Krottner.*
56. 865 F.3d 620 (D.C. Cir. 2017).
57. *Ibid*., note 56, 622.
58. *Ibid*., note 56, 623.
59. *Ibid*., note 56.
60. *Ibid*., note 56.
61. *Ibid*., note 56, 626 (citing *Spokeo*, 136 S.Ct. at 1548).
62. *Ibid*., note 56.
63. *Ibid*., note 56, at 627-8.
64. *Ibid*., note 56.
65. *Ibid*., note 56, 629.
66. 672 F.3d 64 (1st Cir. 2012).
67. *Ibid*., note 66, 69.
68. *Ibid*., note 66.
69. *Ibid*., note 66.
70. *Ibid*., note 66, 70.
71. *Ibid*., at 80.
72. 689 Fed. Appx. 89 (2nd Cir. 2017).
73. *Ibid*., note 72, 90.
74. *Ibid*., note 72.
75. *Ibid*., note 72.
76. *Ibid*., note 72.
77. *Ibid*., note 72.
78. *Ibid*., note 72.
79. 664 F. 3d 38 (3d Cir. 2011).
80. *Ibid*., note 79, 40.
81. *Ibid*., note 79.
82. *Ibid*., note 79.
83. *Ibid.,* note 79.
84. *Ibid.,* note 79.

85. *Ibid.,* note 79, 42.
86. *Ibid.,* note 79.
87. 848 F.3d 262 (4th Cir. 2017).
88. *Ibid.*, note 88, 267–268.
89. *Ibid.*, note 88, 266.
90. *Ibid.*, note 88.
91. *Ibid.*, note 88.
92. *Ibid.*, note 88, 274.
93. *Ibid.*, note 88, 275.
94. *Ibid.*, note 88, 275.
95. 870 F. 3d 763 (8th Cir. 2017) [hereinafter SuperValu].
96. *Ibid.*, note 97, 765–766.
97. *Ibid.*, note 97, 766.
98. *Ibid.*, note 97, 767.
99. *Ibid.*, note 97, 768.
100. *Ibid.*, note 97, 770.
101. *Ibid.*, note 97, 771.
102. *Ibid.*, note 97, 771–772 (the court did, however, find present injury because one plaintiff had experienced fraudulent charges).
103. 'Federal Trade Comm'n, Privacy & Data Security Update (2016)', available at https://www.ftc.gov/reports/privacy-data-security-update-2016#data (accessed 24th January, 2018).
104. 15 U.S.C.§§ 41–58, as amended.
105. *Ibid.*, note 105, § 45(a)(1).
106. *United States v. InMobi Pte Ltd.*, No. 3:16-cv-3474 (N.D. Cal. June 22, 2016), available at https://www.ftc.gov/enforcement/cases-proceedings/152-3203/inmobi-pte-ltd (accessed 24th January, 2018).
107. *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236, 241 (3d Cir. 2015).
108. *Ibid.*, note 108, 241.
109. *Ibid.*, note 108, 241–242.
110. *Ibid.*, note 108, 242.
111. *Ibid.*, note 108
112. *Ibid.*, note 108.
113. *Ibid.*, note 108.
114. *Ibid.*, note 108,
115. *Ibid.*, note 108.
116. *Ibid.*, note 108.
117. *Ibid.*, note 108, 240.
118. *Ibid.*, note 108, 245.
119. *Ibid.*, note 108.
120. *Ibid.*, note 108, 246.
121. *Ibid.*, note 108, 247.
122. *Ibid.*, note 108, 247–248.
123. *Ibid.*, note 108, 248.
124. *Ibid.*, note 108, 249.
125. *Ibid.*, note 108, 256.
126. Notably, payment card association rules require encryption of payment card data.
127. *Ibid.*, note 127, 240–241 (quoting FTC complaint).
128. Daugherty, M. J. (2013), *The Devil Inside The Beltway: The Shocking Expose Of The US Government's Surveillance And Overreach Into Cybersecurity*, Medicine and Small Business, Broadland.
129. Initial Decision, LabMD, F.T.C. No. 9357, at 24 (Nov. 13, 2015), available at https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf (accessed 24th January, 2018).
130. *Ibid.*, note 130, 30; *LabMD v. Fed. Trade Comm'n,* No. 16-16270-D at 3 (11th Cir. Nov. 10, 2016), available at http://f.datasrvr.com/fr1/016/73315/2016_1111.pdf (accessed 24th January, 2018).
131. *LabMD*, No. 16-16270-D at 3.
132. Initial Decision, note 128, 1, 88.
133. *Ibid.*, note 128, 88.
134. *Ibid.*, note 128, 87 (quoting *Int'l Harvester Co.*, 104 F.T.C. 949, n.52 [1984]).
135. Commission Opinion (July 2016), LabMD, F.T.C. No. 9357, at 1, available at https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf (accessed 24th January, 2018).
136. *Ibid.*, note 136, 9.
137. *Ibid.*, note 136, 1.
138. *Ibid.*, note 136, 20.
139. Koo, J. H. (October 2016), 'LabMD Presses Appeals Court on FTC Data Security Case', *Bloomberg BNA*, available at https://www.bna.com/labmd-presses-appeals-n57982078397/ (accessed 24th January, 2018); *LabMD, Inc. v. Fed. Trade Comm'n,* No. 16-16270, oral argument heard on June 22, 2017.
140. See *FTC v. VIZIO, Inc.*, No. 2:17-cv-00758, at 4 (D.N.J. Feb. 6, 2017), available at https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf (accessed 24th January, 2018).
141. *Ibid.*, note 141.
142. *Ibid.*, note 141, 4.
143. *Ibid.*, note 141, 5.
144. *Ibid.*, note 141, 8–9.
145. *Ibid.*, note 141, 8.
146. *Ibid.*, note 141, 9.
147. *FTC v. VIZIO, Inc.*, No. 2:17-cv-00758, at 4 (D.N.J. Feb. 6, 2017), available at https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf (accessed 24th January, 2018).
148. N.Y. Comp. Codes R. & Regs. tit. 23 § 500.17.
149. Commission Regulation 2016/679, 2016 O.J. (L 119) 1, art. 33 (EU).