COUNTERPOINT

AN OFFICIAL PUBLICATION OF THE PENNSYLVANIA DEFENSE INSTITUTE

An Association of Defense Lawyers and Insurance Claims Executives APRIL 2015

Somebody's Watching Me: Defending Data Breach Claims

By Robert J. Cosgrove and Adam J. Gomez[1], Philadelphia PA

I'm just an average man, with an average life; I work from nine to five; hey hell, I pay the price
All I want is to be left alone in my average home; But why do I always feel like I'm in the Twilight Zone?
Somebody's Watching Me (1984) – Rockwell

INTRODUCTION

It took 20 years for Rockwell to be prophetic, but privacy, the right to be left alone,[2] is everywhere in the news. Bar journals scream out on a daily basis the need for attorneys to understand the cybersecurity marketplace and one can't open a newspaper or turn on a television without news of the latest cyber-attack and resultant data breach of a Fortune 500 company. But, with all of this noise, we think it can be difficult for attorneys, insurers and claims professionals to fully appreciate just what's at stake and to understand just what to do about it. In this essay, we hope to explain what's involved in data breach claims and discuss some of the ways in which data breach claims can be litigated.

WHAT THE HECK IS PII?

Any discussion of data breach claims begins with the phrase "personally identifiable information" ("PII").[3] PII is basically information or data that allows an individual to be identified as a particular individual and not as simply part of a group. In the U.S., PII includes an individual's name, gender, contact information, date of birth, marital status and spoken languages. This U.S. definition is narrower than, for example, the definition of PII in the European Union, where PII includes data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning sex or health life.

In the data privacy world, the entity that collects the data is called the "data collector." Once that PII is collected, the business, agency or entity that does something with the PII becomes the "data processor." A data processor can include a third-party entity that is given the PII by the "data collector" to make some use of. In the U.S., the "data collector" has the ultimate obligation both to ensure that PII is not wrongfully disseminated and to ensure that if a breach does occur steps be taken to control the breach. The overlooked reality of PII is that almost any database maintained by any business, agency or entity is going to include PII (even something as simple as the Pennsylvania Defense Institute's customer database or newsletter subscription list).

What then is a data breach? A data breach

continued on page 2

A Brave New World of Cyber War and Hacking Insurance: An Exploration into the Current State of Cyber Insurance

By Scott J. Tredwell[1] and Anthony Canale, McCormick & Priore, P.C., Philadelphia PA

In December of 2014 audiences across the United States were disappointed to learn that Sony Entertainment would not be releasing their controversial film "The Interview". Of course, we all know that Sony ultimately did release the film, but not before it was leaked to the public. It's a strange timeframe. The movie was advertised, withdrawn, leaked, and then released in select theaters amongst fear and hysteria. It's curious that all of this chaos was the result of several cyber attacks. Sony executives were likely screaming, in the words of Seth Rogen's character Aaron Rapoport: "They honey-potted us!" The attack on Sony consisted of threats to personal safety, stolen data, and the disclosure of many embarrassing email threads. It was later determined that the North Korean government was behind the whole debacle, and at that point Sony put "The Interview" back into theaters. A hacker working under the color of a foreign government complicates legal matters, but this incident again brought the damaging effects of a cyber attack

continued on page 6

On The Inside

We encourage comments from our readers
Write: Pennsylvania Defense Institute
P.O. Box 697
Camp Hill, PA 17001
Phone: 800-734-0737 FAX: 800-734-0732
Email: coled01@padefense.org

Michael Tzorfas, Esquire . . . . . Co-Editor
Carol A. VanderWoude, Esquire . . . . . Co-Editor
Matthew Clayberger, Esquire . . . . . Co-Editor
Elizabeth A. Chalik, Esquire . . . . . Co-Editor

Counterpoint has been designed by the Pennsylvania Defense Institute to inform members of developments in defense-related legislation, relevant and significant cases and court decisions, and any other information which is of interest to the membership.

Somebody's Watching Me

continued from page 1

is an incident wherein PII has been lost or subject to unauthorized acquisition, access, disclosure or destruction in a manner that compromises its security, confidentiality or integrity. We like to think of data breaches as rogue hackers breaking into a network under cover of darkness. But that's only one type of data breach. A data breach can occur if a smartphone, tablet or laptop (with, for example, medical records) is lost or even if medical records from a personal injury lawsuit are not properly shredded. If a data breach occurs (and subject to the specifics of local rules), the data collector must disclose the nature of the incident, the type of PII breached, any assistance the data collector is offering to recover the PII, the steps the individual can take to protect against the wrongful use of PII and a point of contact.[4]

WHY SHOULD I CARE?

There are three basic reasons why you need to understand this brave new world:

First, the amount of PII that exists has increased exponentially since 2000.[5] This makes sense when you consider that in 2000, the vast majority of Americans were still using dial-up internet services and the first iPhone was only released in June 2007. As our devices get smaller and faster and our ability to transmit the data through the internet or cell phones grows, the amount of PII collected and stored will only increase.

Second, no matter what efforts are taken, it is almost impossible to prevent a data breach.[6] Data breaches typically occur because of human error (e.g. a mislaid laptop) or a dedicated criminal attack. While you can take steps to minimize your exposure to a data breach (by, for example, creating a privacy program)[7], the reality is that you can no more guarantee that a data breach will not occur than you can eliminate the risk that a plaintiff will slip and fall on ice on even a well plowed driveway.

Third, over the last year, cyber cover has become the next "big" thing. Insurance companies are trying to understand and thereafter issue cyber coverage[8] and the plaintiff's bar is eyeing cyber litigation as its next asbestos.[9] Under such circumstances, failing to understand the risks of PII, data breaches and the potential theories of litigation would be a mistake.

HOW DO YOU MAKE A CASE?

How then do you make a case?[10] We are some time away from the establishment of the archetypal data privacy case, but an examination of recent decisions from throughout the country suggests certain trends in the ways plaintiffs present their claims to avoid their predecessors' pitfalls. More specifically, plaintiffs and their counsel have learned from a host of past dismissals that data privacy claims commonly suffer three legal deficiencies: (1) a lack of standing; (2) an unsuitable or inapplicable theory of recovery; and (3) an indefinite measure of damages. Additionally, at the same time as plaintiffs continue to creatively evolve and refine their claims to avoid these trappings, it appears that the explosion of data privacy litigation in terms of sheer volume has encouraged the courts to focus more on meritorious adjudication than technical compliance.

Standing

It comes as no surprise that the bulk of data privacy jurisprudence focuses on the question of whether victims of allegedly unlawful data collection practices or security breaches have standing to purse their claims in court. In the traditional sense, standing requires the plaintiff to demonstrate "that the challenged conduct has caused [him] *actual injury*."[11] However, in respect of data privacy claims, many plaintiffs commence suit under the auspices that the wrongful collection or dissemination of their private identifiable information *may* cause future harm to their finances or reputations. What plaintiffs usually fail to offer, however, is any evidence that these types of injuries are reasonably likely to occur, much less actually realized. Consequently, the defense of data privacy claims traditionally focused on the plaintiff's lack of standing, and this strategy was largely successful in securing dismissal of the action in that regard.[12]

Until relatively recently, a staple of the defense bar in challenging data privacy claims was found in the United States Court of Appeals for the Third Circuit's decision in *Reilly v. Ceridian Corporation* where the court affirmed dismissal of the plaintiffs' negligence and breach of contract claims on the basis that allegations of possible future injury at some indefinite time are legally insufficient to demonstrate standing.[13] In particular, the court in *Reilly* considered whether employees who had their personal identifiable information stolen after a security breach at a third-party payroll processing company could recover money damages for the chance that their PII could be used to later hijack their identities.[14] In ultimately dismissing the claims, *Reilly* explained that Article III standing requires an "injury-in-fact"; that is, "an invasion of a legally protected interest that is (a) concrete and particularized, *and* (b)

actual or imminent, not conjectural or hypothetical."[15] The court also added that the plaintiffs' claims failed in respect of standing where the breach of security did not create concrete damages "in both a qualitative and temporal sense" that could be "distinguished from merely abstract."[16]

But as unambiguous and ubiquitous as *Reilly* may have been for defense counsel, more recent, high profile litigation has markedly relaxed the "injury-in-fact" standard.[17] For example, the United States District Court for the Northern District of California's decision in *Claridge v. RockYou, Inc.* has become a polestar of sorts for victims of data privacy breaches insofar as the court accepted the argument that PII is a form of consideration exchanged with the defendant so as to facilitate the performance of other contract obligations.[18] In so holding, the court concluded that PII is "exchanged not only for defendant's products and services, but also in exchange for defendant's promise to employ commercially reasonable methods to safeguard the [information] that is exchanged."[19] As a result, the breach of PII constitutes the loss of "some ascertainable but unidentified value and/or property right inherent in the [personal identifiable information]" such that an "injury-in-fact" can be said to have occurred and standing vested in the plaintiffs.[20]

Further, and perhaps more irreverently, the applicability of *Reilly* was all but disregarded in the recent case of *In re. Sony Gaming Networks and Customer Date Security Breach Litigation* where the United States District Court for the Southern District of California elected to supplant the "injury-in-fact" requirement with a "credible threat" standard.[21] In that case, the plaintiffs' commenced suit against Sony when its gaming network was breached by international hackers.[22] Presenting their claims as a class, the plaintiffs argued that standing could be inferred from the fact that their PII was collected by Sony and then disclosed as a result of its negligence in securing the network.[23] Notwithstanding the plaintiffs' inability to demonstrate that any damage had actually occurred as a result of the disclosure of their PII, the court rejected the *Reilly* articulation and instead held that "a plaintiff need only allege a certainly impending injury that is fairly traceable to the defendant's purposed conduct" to withstand a challenge on standing.[24]

As the juxtaposition between *Reilly* and *Claridge* highlights, and the rapid transition to the court's reasoning in *In re. Sony* makes clear, at least some courts throughout the country have found that data privacy litigation is not merely old wine in a new bottle, but rather represents another example where the law must rapidly evolve to accommodate technology. Consequently, if the latter view continues to hold as data privacy concerns grow, it appears that attacks on standing may not be the best way to defend these types of claims.

Theories of Recovery

Recent case law suggests that data privacy claimants have abandoned novel case theories in favor of repurposing tried and true causes of action. For example, using the period of October through December 2013, an analysis of data-related class action lawsuits reveals that even though the majority of litigation concerning data privacy still arises out of federal legislation like the Telephone Consumer Protection Act and the Fair Credit Reporting Act, the most commonly pleaded state-law causes of action have shifted away from deception, unjust enrichment and breach of fiduciary duty to instead focus on standard conversion, breach of contract and negligence.[25]

In respect of the tort of conversion, most data privacy plaintiffs alleging damages as a result of improper data collection argue that the defendant has improvidently profited from use of unlawfully obtained PII. A prime, though unsuccessful[26] example of such claims is found in the case of *In re. iPhone Application Litigation* where a nationwide class of mobile device users brought suit against Apple alleging that, among other things, the company had surreptitiously collected PII like their geolocation data for sale to third-party affiliates.[27] The plaintiffs in *In re iPhone* alleged that their PII and geolocation data was "property capable of exclusive possession" that was inherently valuable to the extent that Apple could profit directly from its sale to third-party affiliates or use it to develop targeted advertisement.[28] Although ultimately unsuccessful in failing to establish this claim, the theory of conversion espoused by the plaintiffs in *In re iPhone* served as an early example of the cause of action in data privacy litigation that today's victims of unlawful data collection have increasingly turned to as a focal allegation.

In addition to conversion, breach of contract has presented itself as a prime theory of recovery in data privacy litigation because the plaintiff's agreement with the defendant obviates the need to establish the rights and responsibilities of the parties with respect to PII, generally. In fact, breach of contract is a uniquely hybrid theory of recovery in data privacy litigation – and therefore quite popular – because it allows the plaintiff to recover for both unsanctioned collection and involuntary disclosure. A seminal example of this hybrid theory was recently articulated in the case of *In re. Google, Inc. Privacy Policy Litigation* where a putative class of every Google account holder between August 2004 and February 2012 argued that Google had breached its privacy policy by implementing an initiative referred to as Emerald Sea.[29] According to the plaintiffs, Emerald Sea was designed to reinvent Google as a social-media advertising company by collecting data from individual Google apps in order to create cross-platform dossier of user data that would then allow third-party advertisers to tailor their advertisements to the specific consumer.[30] Unsurprisingly, Google account holders objected to this use of their PII insofar as Google's original privacy agreement did not provide for the collection of certain types of data by Google-apps, much less the compilation of that data across platforms for sale to unknown third-parties.[31] All told, the court in *In re. Google* ultimately held that these allegations were sufficient to plead a state-law cause of action for breach of contract, and allowed the plaintiffs' claims to survive into discovery.[32]

continued on page 4

Somebody's Watching Me

continued from page 3

Whereas conversion and breach of contract have become standard in unlawful data collection claims, plaintiffs concerned primarily with the consequences of data breaches and disclosure of PII may also turn to common law negligence as a theory of recovery. Generally speaking, data privacy plaintiffs who seek recovery on a theory of negligence assert that the defendant failed to exercise reasonable care in protecting the PII at issue, either by way of inadequate safeguards or lack of timely notification. However, without a uniform standard of care for the protection of PII[33], courts have been left to impart their own states' negligence regimes to hyper-technical questions surrounding the securitization of routers, networks, servers and cloud-based repositories. One such example of negligence at work in data privacy litigation can be found in the case of *In re. TJX Companies Retail Security Breach Litigation,* where the United States Court of Appeal for the First Circuit held that the plaintiffs sufficiently pleaded a *prima facie* case for negligence to the extent that the defendant's retail establishments failed to implement network security features in compliance with those required by the financial institutions that issued its customers' credit and debit cards.[34]

In light of the data surrounding recent privacy litigation, as well as the exemplar cases, it is apparent that plaintiffs claiming damage as a result of the collection or disclosure of their PII are increasingly interested in pursuing recovery under traditional legal theories. In the case of conversion, breach of contract and negligence, specifically, defendants and defense counsel alike must therefore not only be prepared to demonstrate how these legal concepts relate to the plaintiff's specific claims, but also articulate reasons why they are inconsistent with the current state of technology.

Forms of Damages

A corollary to the fact that plaintiffs initially had difficulties in establishing their standing because of indefinite or future injuries is the reality that, at least in some ways, the notion of traditional monetary damages does not fit with data privacy claims. More specifically, even though recent trends suggest that plaintiffs will be allowed to sue for data collection or data breach, they continue to struggle in demonstrating cognizable harm that can be satisfied with a certain specified sum. Of course, this has not necessarily stopped data privacy plaintiffs from pursuing compensatory damages, or even alleging that they should be redressed for unspecified harms or risks. However, those courts that have navigated these disputes and entertained the issue of damages through the initial pleadings phase have suggested that other forms of damages are appropriate in the context of data privacy litigation.

For starters, the United States Court of Appeals for the First Circuit has held plaintiffs may properly pursue so-called "mitigation expenses"; that is, those expenses that victims of data privacy issues incur in order to prevent or cure the adverse effects of having had their personal identifiable information disclosed.[35] In this respect, unsuccessful defendants can expect to reimburse their adversaries for the costs of fraudulent charges, credit monitoring or identity theft insurance.[36] Still, other courts have gone one step further in respect of damages to hold that the breach of privacy agreement may constitute effective rescission of the contract such that the plaintiff is entitled to reimbursement of any and all paid premiums or user fees.[37] Finally, plaintiffs exercising a private right of action under federal or state legislation may be entitled to costs, attorneys' fees or statutory damages on a case-by-case basis.

An appropriate understanding of damages is undoubtedly crucial to a sound defense no matter the nature of a case. But an appreciation of damages in the context of data privacy is arguably more important where many clients have not yet forayed into such litigation and may struggle to grasp their ultimate exposure. Moreover, effective advocacy for alternative dispute resolution or settlement demands competency with respect to the available forms of damages so as to best position clients to quickly and cost-effectively resolve highly public litigation that can often have far-reaching consequences beyond the courtroom.

CHANGES ON THE HORIZON?

The biggest challenge to cyber litigation in the US is that there is not a single privacy framework or law that controls the arena. Most federal action arises out of the Federal Trade Commission, but the scope of the FTC's powers are unclear.[38] Other federal statutes such as the Children's On-line Privacy Protection Act (COPA), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM), Health Insurance Portability and Accountability Act (HIPA) and Family Educational Rights and Privacy Act, a/k/a the Buckley Amendment (FERPA) also have roles to play. On the local level, every state has taken a different approach to handling cyber claims and many states are considering redrafting their current cyber legislation.[39] The 100 pound gorilla in the corner is what the federal government is going to do and whether it is going to create new legislation that preempts the field. This appears to be the White House's intent as set forth in its recent publication C*onsumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*[40], but as of the writing of this piece it is a long way from a White House proposal to the creation of an actual bill that can pass both House and Senate.

CONCLUSION

I always feel like somebody's watching me
I want my privacy
Woh, I always feel like somebody's watching me
Who's playing tricks on me.

Somebody's Watching Me (1984) – Rockwell

In this modern age, where we transmit personally identifiable information almost nonstop, "somebody is [always] watching me." The challenge for lawyers, insurers and claims professionals is

continued on page 6

Somebody's Watching Me

continued from page 4

how to manage the unique challenges presented by PII. Few things in life are certain, but we think it is safe to say that where the opportunity to make money through litigation presents itself, plaintiffs (and their attorneys) will find ways to attempt to make it. The responsibility for minimizing the damage and ensuring that courts and juries do not overreach themselves rests with the defense bar.

ENDNOTES

[1]Robert J. Cosgrove, a CIPM/CIPP-US, is the managing partner of Wade Clark Mulcahy's Philadelphia office. Adam Gomez, a CIPP-EU, is an associate in WCM's Philadelphia office.

[2]"The right to be left alone—the most comprehensive of rights, and the right most valued by a free people." Supreme Court Justice Louis Brandeis, *Olmstead v. U.S.,* 277 U.S. 438 (1928).

[3]*See generally*, *U.S. Private-sector Privacy: Law and Practice for Information Privacy Professionals,* Peter P. Swire and Kenesa Ahmad.

[4]*See generally*, *Foundations of Information Privacy and Data Protection: A Survey of Global* Concepts, Laws and Practices, Peter P. Swire and Kenesa Ahmad.

[5]http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/

[6]http://www.ey.com/Publication/vwLUAssets/EY*Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf*

[8]*See generally*, http://www.insurancejournal.com/news/national/2014/07/14/334442.htm.

[9]*See generally*, https://www.justice.org/membership/litigation-groups.

[10]For purposes of this essay, our focus is on plaintiff claims filed against a data collector. Obviously, government claims or enforcement actions that can arise from a data breach are even more prevalent than third-party claims. We will address these types of claims and how to respond to a data breach in a separate essay.

[11]Black's Law Dictionary (9th ed. 2009), available at Westlaw BLACKS (emphasis added).

[12]*See, e.g. Reilly v. Ceridian Corporation*, 664 F.3d 38 (3d Cir. 2011); *LaCourt v. Specific Media*, 2011 WL 1661532 (C.D. Cal. 2011); *In re. Science Applications International Corp. Backup Tape Data Theft Litigation*, 2014 WL 1858458 (D.C. 2014).

[13]*Reilly*, 664 F.3d at 42.

[14]*Id*. At 43.

[15]*Id*.

[16]*Id*.

[17]*See e.g. In re. Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F.Supp.2d 942 (S.D. Cal. 2014); *Claridge v. RockYou, Inc.*, 785 F. Supp.2d 855 (N.D. Cal. 2014).

[18]*Claridge*, 785 F.Supp.2d at 860-861.

[19]*Id*.

[20]*Id*. At 865.

[21]*In re. Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F.Supp.2d at 962-963.

[22]*Id*. At 962-963.

[23]*Id.*

[24]*Id*. At 963.

[25]Shahin Rothermel & David Zetoony, *Managing Legal Risks: Trends in Data Privacy & Security Class Action Litigation*, February 2014.

[26]Though ultimately unsuccessful in sustaining their conversion claims, one cannot help but speculate that developments in California state law recognizing property interests in personal identifiable information would lead to a different result today.

[27]*In re. iPhone Application Litigation*, 844 F.Supp.2d 1040, 1050-1051 (N.D. Cal. 2012).

[28]*Id*. at 1052.

[29]*In re. Google, Inc. Privacy Policy Litigation*, 2014 WL 3707508 (N.D. Cal. 2014).

[30]*Id*. at 3-4.

[31]*Id*.

[32]*Id*.

[33]President Barack Obama has recently announced his intention to spearhead a federal data privacy framework that has at its heart a Consumer Privacy Bill of Rights. Putting to the side the fact that such a construct is some time in the making, the fact remains that federally standardizing data privacy will in some ways relieve plaintiffs of the burden to demonstrate a reasonable level of care in the industry of data management. *See White House Announces Federal Fata Privacy Framework as Additional Breaches Signal Litigation*, available at <http://blog.wcmlaw.com/2015/01/white-house-announces-federal-data-privacy-framework-as-additional-breaches-signal-litigation/>.

[34]*In re. TJX Companies Retail Security Breach Litigation*, 564 F.3d 489, 494 (1 Cir. 2009).

[35]*See Anderson v. Hannaford Brothers Co.*, 2011 WL 5007175 (1 Cir. 2011).

[36]*Id*.

[37]*See Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11 Cir. 2012).

[38]See*, http://www.thelegalintelligencer.com/id=1202719474359/Third-Circuit-Weighs-Novel-Cybersecurity-Case?slreturn=20150204064430*.

[39]*Compare*, New York's approach as set forth in *Financial Federalism: The Catalytic Role of State Regulators in a Post-Financial Crisis World*, Benjamin M. Lawsky, Superintendent of Financial Services for the State of New York, http://www.dfs.ny.gov/about/speeches_testimony/sp150225.htm with Pennsylvania's Breach of Personal Information Notification Act 73 P.S. §§ 2301, *et seq*.

[40]http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

A Brave New World

continued from page 1

into the limelight.

It is often the case that data stolen from large corporations, such as Sony, contains personal identifiable information that compromises thousands, if not millions, of everyday people's financial well-being. Hackers have taken the upper hand in the technology security struggle. Initially, victimized companies were forced to look to their commercial general liability policies (CGL) for coverage. Insurers have only recently begun to roll out specialized cyber liability policies to supplement the shortcomings of the traditional CGL policy. For those who are left looking for coverage under CGL policies, there are several problems. The body of law on applicable insurance coverage in this area is rapidly developing. Nonetheless, the recently decided matter of *Zurich v. Sony*[1] demonstrates that finding coverage under a CGL policy is still an uphill battle.

The cyber attacks surrounding Sony's "The Interview" are by no means the first bouts that the goliath corporation has had to endure in this Brave New World of Cyber Insurance. By way of background, Sony's "Play Station" system was previously hacked, leading to stolen personally identifiable information, such as credit card numbers.[3] Sony sought defense and indemnification for multiple class action suits brought by the aggrieved credit card holders. In response, Zurich filed a declaratory judgment action seeking a determination that it did not owe coverage, because Sony's alleged claims were the result of their own disclosure of private or confidential information.[4] The parties argued at great length in regards to the meaning of "disclosure." The presiding judge found that disclosure is an action taken by a party, and because Sony was illegally hacked, the disclosure of private and confidential information was not the result of any action or omission on the part of Sony.[5] Therefore, the court held that it would be rewriting the agreement between the parties if coverage could be triggered by the acts of third parties.[6]

Even if the *Sony* opinion is not well received throughout the country, insurance carriers, presumably not wanting to litigate the applicable