2018 Cyber Summit
October 11-12, 2018
New York City

2018 Cyber Litigation Update - Claims & Judicial Inconsistencies on the Rise

I. Standing/Spokeo through the Circuits – No Uniformity in Decisions

In 2016, the Supreme Court in *Spokeo v. Robins* found that plaintiffs alleging violations of statutes that provide a private cause of action and statutory damages must allege a concrete and particularized harm in order to have standing to proceed under Article III. *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). In that ruling, the Court held that Article III standing requires a concrete injury even in the context of a statutory violation.

The Actual Harm Requirement

The Third, Sixth, Seventh, Ninth and D.C. Circuits have all concluded that plaintiffs don't have to wait for their data to actually be misused to sue the company for allegedly failing to adequately protect that information. The Second, Fourth and Eighth Circuits have issued decisions taking the opposite stance. Some courts, like the District Court in California have found that a statutory violation is sufficient to overcome the harm requirement.

No Consistency between State and Federal Courts even interpreting the same law for Actual Harm.

The Second Circuit's summary order in *Vigil v. Take-Two Interactive Software, Inc*. affirmed the dismissal of a class action lawsuit brought in the Southern District of New York under the Illinois Biometric Information Privacy Act[3] ("BIPA") for want of Article III standing because the plaintiffs had failed to allege an injury-in-fact. The court however left the door open for the plaintiffs to attempt to bring their claims in state court without any allegation of actual harm. The Illinois State Appellate court in *Rosenbach v. Six Flags Entm't Corp.* found that "[a]lleging only technical violations of the notice and consent provisions of the statute, as plaintiff did here, does not equate to alleging an adverse effect or harm." Such a holding concluded that while Article III may not apply in state courts the result was the same.

In a different outcome from April of this year, the Seventh Circuit in *Dieffenbach et al. v. Barnes & Noble Inc*., vacated an Illinois District Court's dismissal of a putative class action alleging Barnes & Noble Inc. failed to protect its customers' financial information during a 2012 data breach. The Seventh Circuit ruled that the plaintiffs had sufficiently alleged economic damages in

the form of security costs and lost time, and that the District Court erred in evaluating the plaintiffs' complaint under state, rather than federal, rules.

Data Security v. Privacy

In consumer cases that follow a hacking incident or data security breach, the vast majority of plaintiffs are unable prove damages and are thus out of court. However, privacy claims, such as a violation of the Telephone Consumer Protection Act (TCPA), which restricts the use of automated phone calls and text messages for solicitation purposes, require no harm before substantial penalties are imposed. Specifically, under the TCPA and similar statutes, there is a $500 damages award for each and every occurrence which is increased to $1,500 for any violation found to be willful. If data privacy cases are found to have standing for pure statutory violations with no actual harm, it is anticipated that filings will increase as with privacy cases where the statutory damages drive the filings. Fortunately, however, there is budding case law in FCRA litigation that more than mere hypothetical harm is necessary to establish standing (including the Ninth Circuit, Seventh Circuit, and several district courts).

Predicting the Future

Perhaps increased cyber statutory frameworks and/or minimum penalties will increase the number of "concrete injury" findings, but the cases will depend on statutory language to avoid the fallout from hyper-technical violations (e.g., BIPA requires a finding of being "aggrieved" which seems to require something more than a mere violation).

II. Biometrics

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by his or her intrinsic physical or behavioral traits. Biometric data has been at the center of multiple high profile cases and has posed significant issue for the social media giant, Facebook. Biometric data includes facial recognition, retina scanning, as well as finger and hand scans, among others.

The collection of this data has placed the security of both the government and individuals at risk. The US Office of Personnel Management's (OPM's) databases were accessed by hackers in May 2015 which exposed personal information, including certain biometric data, gathered by OPM for security clearance investigations of millions of current, former, and prospective federal employees and contractors, as well as non-applicant individuals, such as spouses, whose information was submitted as part of background checks. There have been 20 lawsuits in five different states and the District of Columbia against OPM and its private contractor, KeyPoint Government Solutions as a result. *See In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig*., No. 15-1394, MDL No. 2664.

Biometric Information Privacy Laws/Guidance

Recognizing the risk of use and collection of biometric data various privacy laws have emerged. Specifically, the Illinois Biometric Privacy Act, 740 ILCS 14/1 et seq. ("BIPA"). BIPA isn't new and its origin dates back to the early 2000s and a company called Pay By Touch. Pay By Touch promised to "Change the Way the World Pays" with a "biometric" authentication and payment system. The system allowed consumers to link various accounts (credit cards, checking accounts, loyalty programs, etc.) to their fingerprints. Access to those accounts including the ability to make payments was activated by the touch of a finger rather than using cash or a payment card. In March 2008, Pay By Touch ceased all operations following bankruptcy despite receiving over $340 million of investor money.

Pay By Touch's failure lead to BIPA - in law since October 2008. While BIPA was the first state law of its kind when passed by Illinois in 2008, Texas passed a similar law in 2009 called the Capture or Use Biometric Identifier Act. On July 23, 2017, Washington's Biometric Identifiers law ("Washington BI") went into effect. Lawmakers in Alaska, Connecticut, Montana, and New Hampshire, each proposed their own similar laws governing the collection, use, and retention of biometric information. Moreover, California, New York and other states that not have enacted specific biometric privacy laws have still enacted comprehensive privacy laws that regulate biometrics.

BIPA by illustration, creates a framework (consistent with the other similar laws) for other jurisdictions regarding its requirements as to private entities and biometric data. Critical aspects of BIPA are:

1. Requires notice and release for the collecting, capturing, purchasing, or otherwise obtaining a person's biometric identifiers or information. *740 ILCS 14/15(b).*
2. Absent consent an entity cannot sell, lease, trade, disclose or otherwise profit from biometric data (unless required by law). *740 ILCS 14/15(c)-(d).*
3. Additional safeguarding of biometric data is required. *740 ILCS 14/15(e).*
4. Requires a written policy on retention and permanent destruction no longer than 3 years. *740 ILCS 14/15(a).*
5. Provides statutory damages of $1000 or actual damages (whichever greater) per "negligent" violation and $5000 for each intentional or reckless violation or actual damages whichever greater, plus reasonable attorneys' fees, litigation expenses, costs and other relief. *740 ILCS 14/20.*

Biometric Litigation

BIPA class action claims involving facial recognition technology have been filed against Facebook, Snapchat, Shutterfly, and Google based on facial recognition software utilizing users' photographs. *Norberg v. Shutterfly, Inc*., No. 1:15-cv-5351 (N.D. Ill.); *Martinez et al. v. Snapchat Inc.*, No. 2:16-cv-05182 (C.D. Cal.); *Licata v. Facebook, Inc*., Nos. 3:15-cv-03748, 3:15-cv-03749, and 3:15-cv-03747 (N.D. Cal.). Also, a class action was filed against video game manufacturer Take-Two Interactive Software related to the creation of personal avatars. BIPA claims have also arisen from fingerprinting against LA Tan and Palm Beach Tan related to their membership management programs, against the early education provider - Crème de la Crème - for verifying the identity of individuals authorized to pick up children, against rental locker provider Smarte Carte for rental

locker access, and against grocery chain Marianos, related to clocking employee hours. In total, over 30 class actions have been filed since June 2017 based on facial recognition software and fingerprint collection.

The exposure is significant under BIPA and other state laws of its kind. For instance, in the Roundy's supermarket case, *Baron v. Roundy's Supermarkets, Inc*., 2017-CH-03281 (Cook Cty. March 7, 2017) removed *Baron v. Roundy's Supermarkets, Inc.,* No. 17-03588 (N.D. Ill. May 11, 2017), defense counsel stated that the supermarket ''currently has over 10,000 employees who work in grocery stores located in the State of Illinois and who have clocked in and clocked out of their shifts using biometric technology [along with] several hundred or thousand former employees. . .'' resulting in a class recovery of over $7,500,000 if 75% of the potential class participates in the suit. Notice of Removal, *Baron v. Roundy's Supermarkets, Inc.*, No. 17-03588 (N.D. Ill. May 11, 2017). That number may even be conservative as it assumes that the plaintiffs will not demonstrate intentional violations of BIPA (which increases the penalty from $1,000 per violation to $5,000) and also that the Roundy's committed one ''violation'' with respect to each individual plaintiff.

Some suits have been dismissed at the pleading stage, some have settled (the suit against LA Tan settled on a class-wide basis for $1.5 million - agreeing to pay $600,000 in attorney's fees and settling with each class member for between $125 and $150. *Sekura v. LA Tan Enterprises,* No. 2015-ch-16694 (Cook Cty. Dec. 1, 2016).

Defenses to Litigation from Biometrics

As stated above, Article III standing has been the most successful defense to suits alleging improper disclosure or collection of personal information including biometric data. While few, some courts have found that technical violations of BIPA do not give rise to standing without evidence of actual harm. In *McCollough v. Smarte Carte Inc*., based on the defendants collection and use customers' fingerprints as ''keys'' for public lockers without prior written consent, the court dismissed the claims based on plaintiffs' failure to allege an actual and specific injury under Spokeo. The court further held that a mere technical or procedural violation of BIPA was insufficient to grant standing without a showing of an actual injury. *Id.* No. 16-cv-03777 (N.D. Ill. Aug. 1, 2016). Recently, a decision by the Second Circuit upheld a lower court's ruling consistent with *McCollough*, finding that a technical violation of BIPA could not satisfy Spokeo.

But, more recently in *Monroy v. Shutterfly Inc*., the court held that the defendant's collection of biometric information without the plaintiffs' knowledge or consent was sufficient injury-in-fact to give rise to standing. No. 16-cv-10984 (N.D. Ill. Sept. 15, 2017). The court there distinguished *McCullough*, by citing that the defendant in *Monroy* surreptitiously collected and stored the plaintiffs' facial scans without their knowledge or consent. As such, the plaintiffs could credibly allege and invasion of privacy in addition to any technical violation of BIPA.

What constitutes Biometrics

Since the law is not uniform concerning standing, other defenses in addition to standing have emerged. Focus has been placed on whether the scan of a photograph, rather than the scan of a person's face directly, can constitute a biometric identifier. The defendants argue that performing facial recognition on a photograph is simply collecting information derived from biometric identifiers rather than the identifiers themselves, and the practice is thus exempt from BIPA. So far, courts have rejected this argument by holding that biometric identifiers, as used in BIPA, refer to the measurements themselves rather than to medium through which the measurements are collected.

The Problem with Coverage

Because of the significant potential exposure from these suits, insurers can expect policyholders to insist on coverage positions with respect to various policies, including commercial general liability ("CGL"), employment practices liability ("EPLI") and cyber liability insurance policies. Coverage should be determined on a case-by-case basis. There is no one-size-fits-all approach to these claims.

It is unclear how BIPA claims satisfy the "publication" element of the privacy offense under Coverage B's definition in a CGL policy of "personal and advertising injury." To satisfy the privacy offense, BIPA claims must set forth the "oral or written publication, in any manner, of material that violates a person's right of privacy." Without dissemination of an employee's biometric information to a third-party, it seems the "publication" element fails. A series of exclusions should also bar coverage entirely for BIPA claims, either under Coverage A's bodily injury coverage or Coverage B's personal and advertising injury coverage. Specifically, the Recording and Distribution of Material or Information in Violation of Law Exclusion ("violation of law exclusion"); the Employment-Related Practices Exclusion; and the Access or Disclosure of Confidential or Personal Information and Data-Related Liability Exclusion ("disclosure of confidential information exclusion"), which applies to disclosure of a person's confidential or personal information.

EPLI policies are generally not quite as clear. Because they are not standardized, the availability of coverage should come down to the actual exclusions included in the specific policy. Many EPLI policies provide coverage for workplace invasions of privacy under the definition of "wrongful act." But, only some EPLI policies contain provisions similar to the violation of law exclusion.

Cyber liability coverage may be available but will likely not be available for most, depending on the complaint specific allegations. Policyholder lawyers opine that the clearest path to coverage for BIPA violations may be a specialty cyber insurance policy. Some cyber insurance policies do cover privacy breaches in certain circumstances, and some could argue biometric information could theoretically satisfy the policy definition of confidential or personal information protected from disclosure to the public, although cyber insurance is not standardized and it would seem most policies were not intended to cover BIPA type claims.

In a recent trend, seemingly to chase the policy money, Plaintiffs are alleging that employers hire third parties to handle their biometric scanning systems and disclose to or share with them their employees' biometric information. Whether true or not, this will likely be the subject of many a decision on the duty to defend the employer. Depending on the proofs at trial, these allegations could have a significant impact on a cyber insurer's duty to indemnify the employer.

Constitutional Challenges

The constitutionality of BIPA has been challenged in several cases. For instance, in, *In re Facebook Biometric Info. Privacy Litig.*, Facebook argued (among other things) that BIPA constitutes an unconstitutional burden on inner-state commerce. No. 15-cv-03747 (N.D. Cal.). The court initially rejected Facebook's argument that subjecting it to BIPA would violate the dormant commerce clause, which applies when a state tries to regulate economic conduct wholly outside its borders with the goal of protecting local businesses from out-of-state competition. The court stated "This lawsuit is under an Illinois state statute on behalf of Illinois residents who used Facebook in Illinois." Interestingly, the court stated that evidence showed that Facebook can activate or deactivate features for users in specific states when it wants to do so, presumably using geoblocking technology, and thus Facebook would not have to change it practices with respect to users in other states to comply with BIPA. However, in May 2018, the Ninth Circuit agreed to take up Facebook's challenge to the ruling. No definitive ruling has been made as of this publication.

Personal Jurisdiction

BIPA is an Illinois statute, yet Plaintiff's are pursuing non-Illinois companies in Illinois. This would naturally give rise to a personal jurisdiction argument. Thus far, preliminary challenges to the assertion of personal jurisdiction have yielded inconsistent results. For example, in *Gullen*, Facebook argued that it was not subject to personal jurisdiction in Illinois. The court agreed and found that there were no facts to show that the plaintiff's lawsuit arose out of Facebook's contacts with Illinois, as required for the exercise of specific personal jurisdiction. The two main factors in the decision:

1. Facebook had done nothing to establish a relationship with the plaintiff, who alleged that he did not have a Facebook account and never interacted with Facebook; and
2. The mere fact that Facebook operated an interactive website that is accessible in Illinois did not show that it formed sufficient contacts with Illinois related to the lawsuit.

The court rejected the argument that Facebook directed its facial recognition technology to millions of Illinois residents. Because the plaintiff had alleged that Facebook applied its facial recognition technology to "every user-uploaded photo," the court found that any

alleged collection of biometric data was not "targeted" at Illinois residents. (2016 WL 245910).

A different result was reached in *Norberg*. In denying dismissal, the court found that Shutterfly and its subsidiary were subject to specific personal jurisdiction because they:

1. Offered their services to citizens of Illinois.
2. Shipped their products directly to customers in Illinois.
3. Operated websites that offered goods and services in all 50 states.

Additionally, the court noted that there was a "strong interest in adjudicating the matter locally" because "the plaintiff is a private Illinois resident." (2015 WL 9914203.)

If plaintiffs attempt to subject foreign corporations to BIPA lawsuits in Illinois, defendants can seek to challenge the alleged basis of the court's specific jurisdiction under the guidance of the *Gullen* decision. However, an Illinois court might be more willing to find jurisdiction, as in *Norberg*, if the defendants offer goods or services nationwide or in Illinois specifically.

Statute of Limitations

BIPA lacks an express statute of limitations (SOL). This leaves the door open as to what the applicable statute of limitations should be. The SOL could be one year under 735 ILCS 5/13-201, which applies to certain privacy rights such as ''slander, libel, and publication of matter violating the right of privacy.'' The Illinois Right to Privacy Act—which also does not not have a statutory limitations period, has been interpreted as incorporating a one year limitation period. *See Blair v. Nevada Landing Partnership*, 369 Ill. App. 3d 318 (2006). But, courts have held that Section 12-201's is limited only to those privacy torts involving ''publication,'' as specifically listed in the statute. *Johnson v. Northshore Univ. Judge Presiding Healthsystem*, No. 1-10-0399 (Ill. App. Ct. Mar. 31, 2011).

Support exists for a two-year limitations period under 735 ILCS 5/13-202, which applies to both personal injury suits and statutes which provide for a ''statutory penalty.'' An argument could be made that that BIPA's statutory damages—which aware either $1,000 or $5,000 or actual damage constitute a statutory penalty, which is subject to the two-year period under 12-202. Also, the Illinois Consumer Fraud and Deceptive Business Practices Act, is a three-year statute of limitations. 815 ILCS 505/10a(e). The law applies – broadly to improper data collection and usage, including claims brought under the Illinois Personal Information Protection Act.

Plaintiff's will argue that Illinois' ''catch-all'' statute of limitation period of five years is applicable. 735 ILCS 5/13-205. There have been no decisions on this issue to date.

Choice of Law

It has also become clear that parties to a contract or terms of use agreement cannot necessarily rely on choice of law provisions to dictate the outcome of a dispute, as Facebook found in the Northern District of California where the court refused to enforce California law, finding that doing so would be "[c]ontrary to a fundamental policy of Illinois." *In re Facebook Biometric Info. Privacy Litig*., 185 F. Supp. 3d 1155 (NDCA 2016). The court stated "[b]ut if California law is applied, the Illinois policy of protecting its citizens' privacy interests in their biometric data, especially in the context of dealing with 'major national corporations' like Facebook, would be written out of existence." While the law is clearly not settled on this issue, there appears to be a recognition that where states have specifically legislated a privacy right, courts will grant deference to such a right irrespective of the parties' prior agreements.

III. The IoT Issues

The Internet of Things (IoT) encompasses web-enabled devices that collect, send and act on data they acquire from their surrounding environments using embedded sensors, processors and communication hardware, such as: clothes, wearables, thermostats, cars, lights, refrigerators, and more appliances, medical devices, children's toys, baby monitors, etc.

Theories of Liability/Issues on the Rise

Privacy issues/Wearables in the workplace

When information is collected and stored, there is a risk that the data could become compromised. One of the most popular wearable devices is a health monitor, which is worn throughout the day to collect information about sleep, exercise, heart rate, and more. Information is stored in the device's cloud software. Recent research suggests that devices such as Fitbits can be hacked (when the hacker is within close proximity). By focusing on accelerometers and other motion sensors, researchers at the University of Michigan and the University of South Carolina found that it's possible to, among other things, use sound waves at different frequencies to add thousands of steps to a Fitbit.

Wearables "in most cases don't ship with built-in security and so they're vulnerable to being compromised," according to Vinay Anand, vice president of ClearPass Security at Aruba Networks, an enterprise wireless LAN provider. https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html

Because wearables are usually connected to a variety of cloud apps, an organization's BYOD policy may place the risk of compromise even higher. This means that malware and other types of attacks can utilize the wearable as a path to compromise the phone and then the network. The attacker would then have access to legitimate enterprise credentials that would lead to loss of, or the ransom of, sensitive data.

Additionally, organizations that collect but don't carefully anonymize health-related data have effectively acquired what's known aselectronic Protected Health Information (ePHI), which implicates HIPAA. An organization then is subject to the HIPAA requirements just as a hospital would be. This would include the same fines.

This IoT universe presents not only the type of harm presented by compromised personal information, but actual, physical harm. Take, for example, the risks presented by remote manipulation of medical devises (diabetic pumps, pace makers, etc.), hospital beds with an average of 15 internet connected devices, video and security cameras, and vehicles – these threats are real and they are now part of our daily existence.

Strict Product Liability Issues for connected devices-new theory of liability

From a litigation perspective, much of the IoT universe is simply a modern twist on the age old product liability claim involving defective warnings, design, and manufacturing, as well as breach of explicit and implied warranties. The argument is that by failing to incorporate necessary security elements ("privacy by design"), the product is defective as it was foreseeable that the compromise/intrusion could occur. Some examples include:

In Helene Cahen, et al. v. Toyota Motor Corp., et al., No. 16-15496, 9th Cir., 2017 U.S. App. LEXIS 26261 (9th Cir 2017), the 9th Circuit upheld the Northern District of California in dismissing Plaintiffs' claims regarding the defendants alleged knowledge that the vehicles could be hacked, citing numerous research studies and media articles dating back to 2011 that document the electronic security vulnerabilities of defendants' vehicles.

The Court held that "[1]-Vehicle owners lacked U.S. Const. art. III standing to raise breach of warranty, fraud, and Song-Beverly Consumer Warranty Act claims based on allegations that their vehicles were vulnerable to being hacked. They failed to sufficiently allege an injury due to the risk of hacking, as the alleged risks and defects were speculative; [2]-The owners lacked standing to bring claims under California's Unfair Competition Law, Consumers Legal Remedies Act, and False Advertising Law because they failed to sufficiently allege an injury due to overpaying for their vehicles. Allegations that the vehicles were worth less were conclusory and unsupported by any facts; [3]-The owners did not sufficiently allege an injury due to invasion of their privacy, as there were no specific allegations as to why data collected from their vehicles was sensitive or individually identifiable."

In Flynn et al v FCA US LLC, Jeep vehicle owners launched suit in August 2015 after researchers in a controlled experiment were able to hack a Jeep Cherokee and gain control of certain functions. Initially, though dismissing some, the court found that the overpayment and excessive depreciation claims were sufficient to confer standing, though the "increased risk of death or injury" was not a "substantial risk" sufficient to permit standing to sue. In a recent decision (2018 U.S. Dist. LEXIS 111963 (SD IL 2018)), the court certified three state-based classes of drivers in Illinois, Michigan and Missouri led by named plaintiffs Brian Flynn, Michael Keith and George and Kelly

Brown accusing FCA US LLC of designing and installing defective "Uconnect" infotainment systems in Jeep Grand Cherokees and other vehicles that could be hacked and remotely controlled, finding that there were sufficient facts and evidence to permit the consumers' fraud and warranty claims to proceed. The judge did not certify a nationwide class, holding that "it would be unwieldy and require highly individualized inquiries" to sort through the underlying state laws governing the implied warranty, fraud and products-liability claims at issue."

Home security company ADT paid $16 million dollars to conclude five proposed class actions arising from it's failure to disclose known security flaws. In one of them, *Edenborough v. ADT LLC*, case number 3:16-cv-02233, in the U.S. District Court for the Northern District of California, Plaintiff argued that the company was fully aware that the wireless security systems were vulnerable to disruption because they lacked encryption, and disclosed in a 2016 SEC filing that some of its devices may be subject to hacking. While some claims were dismissed, the court concluded that fraudulent omission claims could proceed. In another, *Baker v. ADT LLC* in the Central District of Illinois, strict product liability claims were dismissed (among others), barred by the economic loss rule, presenting an interesting defense where there is purely an economic harm alleged, but the court permitted the case to proceed on other grounds, including consumer protection statutes and common law unjust enrichment. Thus, for varying reasons, the IoT universe of claims often present a wide variety of legal theories which courts are reluctant to dismiss.

In, *In re: VTech Data Breach Litigation*, case number 1:15-cv-10889, in the U.S. District Court for the Northern District of Illinois, VTech was successful in seeking dismissal of claims against it arising from data breach which occurred involving the company's app store on both standing grounds and, following amendment of the complaint, for the failure to establish the "overpayment" theory – that the Plaintiffs did not receive the benefit of the bargain in what they paid for the toy.

Thus, in this developing body of legal precedent, IoT litigation presents an expanded means of pursuing claims arising from potentially flawed data security and privacy protections.

Medical Devices

There are no reported instances of a medical implant device, like a pacemaker being hacked in order to hurt the person, but it could happen as has been demonstrated by penetration testing. However, what appears a larger target of digital trespassers is hacking a device, like a networked MRI machine as a way into a Wi-Fi network. Such would provide access to a health system's network, ultimately risking patient safety by potentially interrupting care by holding electronic health records hostage; breaching

protected health information; taking down the system entirely; or simply causing devices to malfunction.

Healthcare organizations must be concerned about the security of their devices—both those installed in hospitals and those installed in patients themselves. Keeping cyber intruders on the outside is a difficult task. It requires training health system employees from the C-suite down, putting devices on secure parts of Wi-Fi networks, and keeping an eye on smaller issues, like default logins.

Uptick "Swatting" cases

Swatting is an internet prank/crime where someone finds an address either through an IP or because the person's name and location is known. A 911 call is placed anonymously and reports a fake emergency. For instance, the caller can say that someone at that address is being held at a gun point or someone is going to commit suicide and a SWAT team would be dispatched to the address.

Cybercriminals use a variety of technical maneuvers to make it appear as if the prank call to police originated at the residence of the unsuspecting victim. Police, with no choice but to react to the crime, often send out SWAT teams, bomb squads, and other emergency services such as fire trucks and ambulances.

Most swatting attempts target gamers who broadcast their gameplay on live-streaming services but celebrities such as Tom Cruise, Miley Cyrus, and Justin Bieber have all been "swatted" as well.

"Jackpotting" ATM machines

Jackpotting is a malicious cyberattack that has the U.S. Secret Service issuing warnings and banks on high alert. It is a method by which criminals use hacking tools to force ATMs to spit out thousands of dollars in cash. While jackpotting has been around for years, its first verified cases in the U.S. were reported in early January 2018. https://krebsonsecurity.com/2018/01/first-jackpotting-attacks-hit-u-s-atms/

Jackpot schemes, also called "logical attacks," have threatened European and Asian banks but not U.S. banks.
https://www.sacbee.com/news/business/article197070159.html#storylink=cpy

A 2016 report by Bank Info Security regarding jackpotting in Europe said hackers can steal the cash without physical contact with the ATMs, using just a mobile phone. However, according to the Krebs' report, the jackpotting attacks do require physical access, as well as malware and sometimes a device called an endoscope, which physicians use to observe the inside of the human body.

Driverless cars

Oscar Nilsson sued GM in U.S. District Court in January for negligence over a December 2017 crash in which he was injured. Nilsson's suit claimed the self-driving GM Cruise "suddenly veered back" into Nilsson's lane, striking him and knocking him to the ground. GM's report on the crash to California regulators said the car was operating in heavy traffic, when it saw a space between two vehicles in the left lane and began to merge. At the same time, a vehicle decelerated and the self-driving car stopped making the lane change and returned to the center lane.

As the Cruise was re-centering itself, the motorcyclist that had just lane-split between two vehicles in the center and right lanes moved into the center lane, glanced the side of the Cruise, wobbled, and fell over, the report said. GM said a police report found Nilsson at fault for attempting to overtake and pass the Cruise, but Nilsson's lawyer said he was not issued a citation in the incident. The case centered around traditional principles of negligence between motorists. *Nilsson v. General Motors* (CA).

Flynn v. FCA US (SD IL), outlined above, was one of several "car hacking" class actions filed in 2015 following a series of well publicized media reports concerning the "hackability" of certain cars through their infotainment systems. Plaintiffs articulated an "overpayment" theory of damages premised on the notion that purchasers reasonably expected and paid for information security when they purchased Chryslers, and are therefore entitled to recover that percentage of the sales price attributable to information security because of the security flaws in the UConnect system. Similar overpayment theories have been attempted in data breach cases, including the Target class action and *Cahen*, but have been rejected by courts on the grounds there is no reasonable basis to believe consumers considered data security when they made their purchasing decisions. *Flynn*, the first car hacking case to proceed to trial on a class wide basis, is also the first data security case to proceed past summary judgment *in which no actual breach had occurred*. The *Flynn* plaintiffs' damages theories relied on conjoint analysis, a branch of marketing theory which postulates that a value can be placed on consumer expectations at the time they make purchasing decisions, raising significant potential impacts on future IoT litigation.

IV. Cyber E&O Claims

Impleading cloud providers-risk transfer

The cloud offers a way to offload some IT functions that require significant security and compliance investments to a vendor. Ultimately, however, the company is still responsible for its customers' data wherever it resides. Underappreciated is the fact the even when the a data privacy incident arises from data stored by a cloud provider, it is difficult if not impossible to achieve any monetary contribution from the provider for the costs of the data privacy event –whether remediation, breach costs or consequential damages.

Whether cloud hosted or not, the key element of an IT security management is risk management and ultimately IT security management is the foundation upon which breach costs can be offset, avoided or transferred. Effective risk management guarantees the required security and simultaneously allows the effective use of resources. The cloud computing model entails specific types of risk, which results from the type of resources that can be threatened, as well as technologies. The key element of the risk management process is the risk analysis and then implement a risk management procedure. A risk management procedure should:

1. identify the methods, tools and means of risk reduction and transfer, as well as estimate their cost and effectiveness;
2. implement the methods and means of risk reduction or transfer,
3. determine the acceptable level of risk;
4. establish the methods of risk avoidance.

Focusing on risk transfer as a critical aspect of a risk management procedure. The transfer of risk consists of transferring the consequences of damage occurrence or the financial liabilities resulting from a data privacy event on another entity (i.e cloud provider). The fundamental rule of such an operation is transferring the consequences or liabilities on an entity which is able to manage its risk better than the entity which wants to eliminate this risk or reduce it. The forms of risk transfer in organizations include outsourcing or insurance. Outsourcing the IT responsibility may transfer responsibility in a theoretical sense, but in a legal sense the risk may not actually be transferred.

Impediments to successful risk transfer involve lack of access to critical information to determine the cause of the data privacy event and ineffective contract terms for indemnification. The key to overcoming both impediments is a comprehensive, written contract between the company and the cloud vendor which details all applicable service level expectations and other important duties each party must effectively perform.

While vast and detailed in terminology, at its core, the agreement should clearly define both the company's and the cloud provider's roles and responsibilities. In order to effectively transfer the risk the following minimum terms are necessary in a written agreement with the cloud service provider:

1. Compliance – the agreement must assure that all systems and subsystems which will process, store or otherwise record protected information as defined and governed by any local, state, or national regulations.
2. Electronic Discovery (ESI) – the agreement must require the cloud provide to preserve and produce, at the company's request, any ESI contained on their systems and networks.
3. Data Ownership – the contract should state clearly that company retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement.
4. Composite Services and Control over Subcontracting – cloud services themselves can be composed through nesting and layering with other cloud

services and providers. Cloud service agreements should contain a clause that defines the scope of control over the third party, the responsibilities involved and the remedies and recourse available should problems occur.

5. Right to Audit –the company must have the right to audit the cloud provider and any subcontractors for compliance with contractual obligations, at the company's sole discretion.
6. Transparency and Cooperation – to ensure that policy and procedures are being enforced throughout the system, the cloud service agreement should include some means for the company to gain visibility into the security controls and processes employed by the cloud provider and their performance over time.
7. Indemnification and Limitation of Liability – though the proliferation of cloud service providers is creating sufficient leverage for knowledgeable buyers to obtain more agreeable contract terms, most agreements still contain one-sided clauses that deny indemnification to the sourcing department by the cloud service provider, even for situations where the provider is solely negligent for an adverse event's direct and/or consequential damages. In other instances, the provider may agree to indemnify for loss, damages, and expenses caused entirely or aggravated by the negligence of the provider. However, such is often coupled with a limitation of liability that caps economic damages owed to no more than the notional value of the contract. It is critical that the agreement not contain any language that eliminates or reduces the provider's obligation to indemnify the company for loss or damage caused by its negligence nor contain language that caps or limits its obligations for the full financial liabilities arising out of such negligent act or action.
8. Insurance – commercial insurance can serve that vital role in assuring the company has access to financial resources needed to deal with the consequences of a casualty arising out of the cloud provider relationship. A clause should be included in the provider agreement that mandates the cloud provider maintain, as a minimum for the life of the agreement, a minimum amount ($3 million is considered commercially reasonable) of so-called cyber liability insurance in addition to the standard types and amounts of coverage required by company of all other goods & services vendors.

For an example, see Harvard's Cloud Service Provider Requirements. https://rmas.fad.harvard.edu/cloud-service-providers.

Unless you can establish causation of a breach, which is generally impossible unless you have access to the data (now stored with the cloud provider) along with the ability to conduct forensics, impleading a cloud provider will be fruitless endeavor. Further, without the appropriate indemnification language, a company/carrier seeking reimbursement from a cloud provider may be left with no legal remedy.

Professional Liability Claims

Professional firms represent some of the most frequent targets of a cybersecurity breach. Lawyers, accountants, real estate professionals, property managers, etc., all possess vast amounts of private information and remain exclusively reliant on web-based services to operate their businesses. These factors, along with often lax data security programs, create the ideal environment for data breaches, ransomware events, social engineering and business email compromise claims, as well as other consequential damages, such as the inevitable and often very expensive business interruption claim. Increasingly creative Plaintiffs are arguing that such breaches constitute not only professional negligence, but a breach of fiduciary obligations, express and/or implied contracts and overpayment for services provided. In light of the vast number of outside vendors interacting with these firms on a daily basis, as well as the increased popularity in using artificial intelligence as a means of decreasing operational costs, professional firms also face significant exposure from the involvement of third-parties potentially exposing their systems to intrusion.

Coverage/Crime/Fidelity Issues

Where an insured does not have a stand alone cyber insurance policy, much recent litigation has centered on whether coverage arises from other forms of coverage, such as crime and fidelity policies. For example:

- Apache Corp. v. Great American Ins. Co.,: 2016 - Fifth Circuit ruled that loss resulting from fraudulent e-mail did not trigger coverage under crime policy "computer fraud" coverage because the loss was not the "direct result" of computer use
- Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co. of America: 2016 - Ninth Circuit affirmed summary judgment in favor of Travelers Casualty and Surety Company of America in an insurance dispute concerning the applicability of computer fraud coverage to a fraudulent wire transfer incident (hacker posing as vendor) resulting in over $700,000 in losses to Seattle-based seafood importer Aqua Star (USA) Corp. - policy exclusion for loss resulting from authorized access.
- Taylor & Lieberman v. Fed. Ins. Co.: 2017 - Ninth Circuit finds no coverage under crime policy for client funds lost in social engineering fraud
- Medidata Solutions, Inc. v. Federal Ins. Co.,: July, 2018 - Second Circuit, applying New York law, affirmed a district court ruling that the computer fraud provisions of a commercial crime coverage section covered the losses Medidata incurred when the company's employees transferred funds in response to a spoofed email.

Cyber D&O Claims - Securities Class Actions

Over the past year, several federal class action securities fraud lawsuits against public companies have been filed after data security incidents. The core issue in securities fraud litigation is often whether the public company made a material misrepresentation or omission that deceived the market = What companies say about data security in their SEC filings, press releases, and other communications is critical. This typically involves one of two legal theories in arguing that a company's stock was artificially inflated: First,

shareholders have alleged that the company's pre-breach public disclosures didn't adequately disclose the risk (*Ali v. Intel Corp.; Kim v. Advanced Micro Devices, Inc.) of* a data security incident or that the company overstated its cybersecurity strength or capabilities (YAHOO; Equifax). Second, that the company withheld or was too slow in disclosing a breach after it was detected. Ultimatly, this represents a shift in Plaintiffs' strategy: Shareholder derivative suits (shareholder sues the board on the company's behalf based a fiduciary duty claim) haven't gotten much traction. The bar for such lawsuits is high since directors are protected by the business judgment rule and shareholders must show that the board "completely failed" or "consciously failed" to exercise its oversight responsibilities.