The Harmonie Group
2018 London Seminar
Wednesday, 17 October 2018

Program Emcee: Michael Howard

Who's To Blame?
Tips for Early Identification of Subrogation and Potentially Liable Parties

Patricia A. Lawson, Adam Grant, and Stephanie A. Sales
McCague Borlack, LLP

Introduction

In order to determine whether or not subrogation is a viable option with respect to any loss, it is first necessary to consider the cause of the loss, followed closely by who is responsible for the loss.

In the instance of a fire caused entirely by the negligence of the insured, there is no wrong-doer or tortfeasor to sue. An example might include where the insured knocks over a candle that he or she lit or where the Insured leaves a pot of oil on a stove unattended causing a fire. The circumstances change if the Insured knocks over a candle that he or she did not light and did not know was lit or if the Insured leaves a pot of oil on a stove when all of the elements are in the off position. The question then becomes: How did the fire start and who is liable for the resulting fire damage?

Initial Investigation

When a loss occurs and there is any indication that it might have been caused by a product failure or the negligence of someone other than the insured, it would be prudent to obtain a report with respect to its cause as quickly as possible. Having an expert perform an examination shortly following a loss will make it more likely that the expert will have access to evidence necessary for the purposes of analyzing the cause of the loss. Moreover, the expert's final report will be instructive in determining the identities of parties who should be included in the claim.

This is especially critical in losses such as fires, where the entirety of the evidence as to the cause of the loss can be easily disturbed, and must necessarily be destroyed in order to repair the damage.

The importance of identifying all potentially liable parties when contemplating subrogation cannot be overstated. In Ontario, the basic limitation period in which to start a claim is two years from the day on which the claim was discovered.[1][2]

It is therefore imperative that all potentially liable parties are identified as quickly as possible following a loss and well in advance of two years from the date on which the loss occurred. Early identification of potentially liable parties also increases the prospect of early settlement discussions in a matter and potential resolution, as well as assisting in identifying evidence that should be preserved in order to prove the claim.

Fires

In cases of fire that begin following the work of a contractor or subcontractor, where it appears that the fire began as a result of that work or during that work, it is important to identify the party with whom the insured contracted for the work and the party whose negligence caused the fire. With respect to the work of the party with whom the insured contracted, the claim against the contractor

[1] *Limitations Act*, 2002, S.O. 2002, c. 24, Sched. B.
[2] Generally speaking, the date of loss should be treated as the date on which the claim was discovered for the purposes of setting a limitation period. However, each case must be considered on its facts.

may be pleaded in contract, in that the contract was breached, and in negligence. With respect to the work of any party who caused the fire, a claim for negligence may be made.

It is essential that the party with whom the insured contracted is included as a Defendant in the claim. That party arguably had a duty to carry out the work competently and lawfully and to contract with competent subcontractors or employ competent agents, servants and/or employees in execution of the work.

Although pursuing the contractor alone is generally sufficient, it is often advisable to include the subcontractor. First of all, the Defendant contractor has no obligation to start a third party action against the subcontractor. Where the Defendant decides to do so, the process can be a lengthy one and will usually delay progress in the main action.

If the Defendant contractor cannot be found or does not have insurance, it may be impossible, in the former instance, or difficult, in the latter, to recover any amount for damages from the contractor.

Finally, by including the subcontractor in the claim, it is more likely that the parties will be able to obtain all relevant documents pertaining to the action. It also provides the insured with an opportunity to examine the subcontractor for discovery which may assist in proving the claim against one or both of the tortfeasors.

Where there are several subcontractors involved in a project during which a fire is caused, it is generally prudent to include all of them in the claim for the reasons above.

Floods

In cases of flooding or water damage, there are several parties who may be liable for the damages caused, depending on the source of the water escape. For example, where a flexible connector is involved, the parties who may bear some responsibility include the manufacturer of the connector, the plumbing contractor who installed it, the plumbing contractor who repaired or serviced it subsequent to its installation and the home builder who sold the property to the insured in the first place.

In all product failures, a claim may be asserted directly as against the person who sold the defective item to the insured[3], but it remains prudent to investigate the entire supply chain, and name all parties through whom the product passed. The manufacturer of the product has an obvious level of exposure to the claim, but vendors in the supply chain may also have exposure if they did or should have conducted tests of the defective product, or if they were in a position to have warned users of the product.

Failure to Prevent/Mitigate

The avenue to subrogation is obvious where a party may have been directly responsible for causing the loss, but there remain other avenues of subrogation that can be pursued. In the case of defective workmanship, consideration should be given to any parties who had an obligation to inspect such workmanship. This can include architects or engineers, construction managers, municipal inspectors, administrative authorities, etc. Although these parties often had no part in directly

[3] *Sale of Goods Act*, R.S.O. 1990, c. S-1

causing the loss, they may have been in a position to discover the defective workmanship which ultimately caused the failure, and can be held liable for this.

Likewise, after a loss has occurred, a number of parties are responsible for mitigating the loss, such as emergency and security personnel, and those responsible for automatic mitigation systems such as sprinklers. In the event that the immediate response to the loss is not as effective as expected, there may be available avenues to pursue these parties for failure to properly respond to the loss. While actions as against emergency services such as fire departments can be difficult to succeed in, actions as against security companies, and parties responsible for the design and construction of fire suppression systems can be very lucrative.

Unfortunately, this class of subrogation target will often not be held liable for the full extent of the loss, as they ultimately did not cause it. However, when more direct targets are not available, or have insufficient insurance coverage, pursuing these targets can greatly increase the recovery potential.

Conclusion

The initial investigation following a loss is a crucial. Obtaining a statement from the insured and anyone else who is aware of the circumstances giving rise to the loss at the outset will ensure that that evidence is preserved over time as memories fade. Physical evidence should also be identified and preserved immediately. Consideration should be given to whether or not an expert's report is necessary in order to determine what caused the loss, the identities of potentially liable parties and, inevitably, assisting in proving the claim if the matter proceeds to litigation.

Adam Grant
McCague Borlack LLP
Suite 2700, The Exchange Tower
130 King Street West
Toronto, ON M5X 1C7 Canada
(416) 862-8631
agrant@mccagueborlack.com

Patricia A. Lawson
Stephanie A. Sales
McCague Borlack, LLP

Spoliation 101

Irina Sfranciog
Mccague Borlack LLP

The Basics: What is Spoliation?

The doctrine of spoliation in Canada has evolved from the English common law[1]. Spoliation refers to a rule of evidence when there is tampering, destruction, alteration or concealment of evidence. Issues of spoliation arise most often in subrogation claims when evidence has been lost or destroyed. In Canada, spoliation is also recognized as an independent, stand-alone tort.[2]

Spoliation occurs where a party has intentionally destroyed evidence relevant to current or contemplated litigation and a reasonable inference can be drawn that the evidence was destroyed in order to affect the litigation.[3]

All types of evidence can be subject to spoliation and spoliation can occur in various ways. For example, spoliation can occur when documents are shredded, emails are erased, physical evidence is sold, destroyed or hidden, and in circumstances where evidence is otherwise rendered unavailable for trial. The doctrine of spoliation becomes especially important in matters involving electronic discovery of evidence. With the simple click of a mouse, electronic evidence such as an email can be permanently deleted. Often times, electronic records such as emails or text messages are notoriously difficult to retrieve since parties often clear their inboxes or delete messages they think they may not need again.

As we move towards a "paperless" society where the destruction of physical documents becomes routine, it is important to remain cognizant of the difference between simple, routing shredding of documents and the intentional destruction of documents relevant to existing or pending litigation.

Intentional vs. Unintentional Spoliation

In situations where evidence is destroyed by accident, does spoliation still arise? The short answer is no. The Ontario Superior Court of Justice has articulated that the following four elements must be established on a balance of probabilities in order to find that spoliation has taken place:

1) The missing evidence must be *relevant*;
2) The missing evidence must have been destroyed *intentionally*;
3) At the time of destruction, *litigation must have been ongoing or contemplated*; and,
4) It must be *reasonable to infer* that the evidence was destroyed in order to affect the outcome of the litigation.[4]

In addition to the above, the Ontario Superior Court of Justice also found that there must be evidence that *a particular piece* of evidence was destroyed.

[1] *Armory v Delamirie [1722] EWHC J94*.
[2] *Spasic Estate v Imperial Tobacco Ltd.*, 2000 CanLII 17170 (ON CA).
[3] *St. Louis v R.* (1896), 25 S.C.R. 649 (S.C.C.))
[4] *Nova Growth Corp. v Kepinski*, [2014] ONSC 2763 at para 296.

It is also important to draw a distinction between spoliation as a legal concept and spoliation as a common sense concept. The destruction of evidence on its own is not sufficient to trigger the adverse inferences that can be made by a Court when spoliation is found. There must also be intent to destroy the evidence for the purpose of affecting the litigation.

Consequences of Spoliation

In Ontario, Courts derive their power to impose sanctions on spoliators by virtue of their inherent jurisdiction and from the *Rules of Civil Procedure*. It is generally incumbent on the party pleading spoliation to request that the Court impose sanctions.

The Court's inherent power to find adverse inference serves three basic functions:

1) Deters spoliators
2) Promotes accuracy
3) Compensates victims of spoliation

Once spoliation is established, the Court *presumes* the evidence would have been unfavourable to the party who destroyed it.[5] Courts are able to draw an adverse inference against parties that spoliate evidence. In other words, when applied, spoliation of evidence gives rise to a rebuttable presumption of fact that the missing evidence, had it been preserved, would have been unfavourable to the party that destroyed it. Courts can also make an adverse inference that the spoliator had some motivation to destroy the evidence (i.e. the email was deleted *because* it was unfavourable). Once a Court finds that intentional spoliation has taken place, the spoliator faces an uphill battle in that the Court can conclude that the evidence that was spoliated would have been unfavourable to the spoliator.

Although Courts generally draw an adverse inference in situation where evidence has been intentionally destroyed, sanctions may also be imposed for the unintentional destruction of evidence. For example: Courts can impose sanctions on a party that destroys evidence when that party *knew or ought to have known* that the evidence was relevant to existing *or* pending litigation. In other words, parties in Canada can be sanctioned by Courts for destroying evidence recklessly, or inadvertently through negligence.

These sanctions can be applied in the form of costs, preclusion of evidence and in rare circumstances, even dismissal of an entire action. However, it should be noted that there is a very high threshold for the imposition of a sanction dismissing an entire action. The primary remedy for spoliation is the imposition of the rebuttable presumption of fact that the lost or destroyed evidence would not assist the spoliator at trial. This presumption can be rebutted by evidence that shows the spoliator did not intend, by destroying the evidence, to affect the litigation.

On the present state of the law in Canada, it is clear that spoliation requires <u>intentional</u> conduct (i.e. the evidence in question was destroyed with the knowledge that the evidence would be required for litigation purposes). When the destruction is not intentional, it is not possible to draw the inference that the evidence would tell against the person who has destroyed it.[6] Examples of unintentional spoliation includes: video surveillance of a loss or incident that is automatically erased every 30 days.

[5] *McDougall v Black & Decker Canada Inc.*, 2008 ABCA 353 at para. 18.
[6] *McDougall v Black & Decker Canada Inc.*, 2008 ABCA 353 at para. 24.

Who Spoliated the Evidence?

Issues involving spoliation are very common when subrogation is considered by an insurer after a loss. The prospect of successful subrogation hinges almost entirely on the strength of the direct or circumstantial evidence available to establish 1) liability and 2) damages. Spoliation can take place when evidence is destroyed by the insurer, insured or a third party. In situations where evidence is spoliated by the insured, the insurer will have little recourse since it cannot subrogate against its own insured. If the evidence in question is spoliated by the insurer, the opportunity to subrogate can be lost entirely and an adverse inference will likely be imposed on the insurer in a subrogated action since it has a real interest in the subrogated action. If the evidence is spoliated by a third party however, then the insurer would be in a position to seek an adverse inference to be made by the Court against that third party.

Takeaway for Subrogation Claims

The key to avoiding spoliation is preservation. From the early stages of a claim, adjusters should attempt preserve all the evidence possible from the outset of a loss, even if the evidence does not appear to be relevant at that time.

For example, in property damage cases, before any remediation or repairs take place following a loss, it would be prudent, at the very least, to take photographs of all evidence and try to preserve as much physical evidence as possible. In subrogated claims where property damage is usually at issue, hiring an expert origin and cause engineer from the outset in order to preserve and store evidence is crucial. In addition, any destructive testing should be put on hold until the third party has been put on notice and has been provided with an opportunity to attend the proposed destructive testing.

In fire or water losses arising from a defective component or part, preserving physical evidence is often the only way to ensure that no adverse inferences are drawn and that no sanctions (i.e. costs) are awarded against the party. It is rare that an insured will independently anticipate litigation and retain evidence in order to assist an insurer in any subrogation efforts. An insured may look at a failed electrical or plumbing component as garbage and simply throw it away. However, without a closer examination as to the cause of failure, potential recovery is disregarded from the outset and so are any possibilities to subrogate. Indeed, it may very well be the case that the electrical or plumbing component in question is the subject of a recall or failed due to a manufacturing defect. Although it may at times be difficult to determine what evidence is relevant during the initial investigation of a loss, communication with the insureds from the outset of the claim with respect to retaining and preserving all evidence can go a long way.

Subrogation and Assessment of Claims

Adam Grant
McCague Borlack, LLP

Subrogation is the mechanism by which an insurer can recover monies that it has paid to its insured by bringing an action in the name of the insured as against a third party who is responsible for the loss.

The right of subrogation is established contractually, at common law, and in section 278(1) of the *Insurance Act*. Most insurance policies contain language which broadens the right of subrogation beyond that granted by statute and common law.

When can the Insurer Pursue Subrogation?

At law, the insurer's right of subrogation arises only when the insurer has paid the insured for some portion of its loss. Moreover, until the insured is completely indemnified for all insured and uninsured losses, the insured has the right to control the action.[1] In order to give the insurer command over a subrogation action, standard terms of the insurance policy will often contain language that stipulates that the right of subrogation is triggered as soon as the insurer assumes liability for a loss, rather than once the insurer has paid any portion of the loss. This wording will also often give the insurer the sole right to control the action, and settle claims without the insured's instructions.

Occasionally, the insured may also initiate an action against the same third party. If both the insurer and the insured commence separate actions, the rule against multiplicity of actions may prevent one of the actions from proceeding. Insurers need to be mindful of this possibility and alert the insured of their intent to pursue a claim in order to prevent the failure of their action.

Where the insured does pursue its own claim, it has an obligation to protect the subrogated interest of the insurer. Likewise, the insurer is obligated to protect any uninsured interest of the insured in its subrogated actions.

What Claims are Suitable for Subrogation?

Not all payouts by an insurer for insured losses are fit for litigation and determining what claims are appropriate to pursue is not always a quick or easy task. Some subrogation opportunities are not obvious and will require investigation and creative thinking.

The insurer's first step, after determining the cause of the loss, is to determine who the potential wrongdoers are. In simple terms, the insurer should consider what, if any, third party could be responsible for the wrongdoing. In legal terms, this party would be liable for the loss. Liability describes the state of being actually or potentially subject to a legal obligation.

Some questions to consider in the determination of liability include:

- Who had last access to the area or the product?
- Who manufactured the product?

[1] *Zurich Insurance Company Ltd v Ison TH Auto Sales Inc,* 2011 ONSC 1870 (CanLII).

- Who was the supplier?
- Who did the installation? Was it a contractor, or a subcontractor?
- Who was responsible for maintenance?
- Was there a contract?

Beyond this, the insurer should then examine if and how the loss could have been prevented entirely. One consideration is if the parties could have foreseen the problem prior to the loss. This involves further questions, including:

- Could the problem have been noticed during movement through the supply chain from the manufacturer to the retailer?
- Was there something that could have been done during the design, installation, inspection, and/or maintenance steps that could have identified a deficiency or prevented the loss?
- Was municipal and/or administrative approval obtained?

The insurer should then consider whether parties may have been able to mitigate the loss. These parties would not be responsible for the entire loss, but may be responsible for some portion of it, as they could have prevented the damage being as significant as it was. Among the questions to ask include:

- Was the emergency response adequate?
- Was the suppression/alarm system designed and/or functioning properly?
- Was there adequate security present in the area?

Example: Sprinkler Systems

Sprinkler system failure is a relatively common cause of water damage, and nearly always yields subrogation potential. Failure of the system is almost always due to freezing and bursting of the lines. However, the insurer should not rush to blame cold weather for these freeze-ups.

Wet sprinkler systems are only permitted for use in heated spaces. They should therefore not be able to freeze. There a number of reasons for why a sprinkler system may fail, including inappropriate heating levels, improper design and/or construction of the building envelope, an improperly designed, built, and/or inspected sprinkler system, and the failure to conduct annual inspections. Simply put, wet sprinkler systems should be protected from freeze-ups. If one does freeze, someone has likely done something improper, leading to the failure.

The same holds true for dry sprinkler systems. These systems are intended for unheated spaces, so they contain pressurized air instead of water. If one of these systems fails as a result of a freeze-up, the insurer should consider how the water got into the system, whether the sprinkler was designed and/or constructed with a proper slope, whether the sprinkler system was properly inspected, and whether annual inspections were completed in order to determine what led to the failure. The answers to these questions could identify one or more parties liable for the failure of the sprinkler system.

Establishing Liability
To establish liability at law, the insurer must prove that the third party breached a responsibility they owed to the insured. The most common way to establish this breach is to pursue a claim in negligence.

To succeed in a negligence claim, the insurer must show, on a balance of probabilities, that:

1. The wrongdoer had a duty of care/responsibility to the insured;
2. There was a breach of the standard of care;
3. The wrongdoer caused that breach; and
4. The insured suffered damages.

However, should a successful claim in negligence be unavailable, liability can also be established through breach of contract. The insurer should consider whether a party was required to complete work under a contract, including general contractors, property managers, security providers, or other work falling under the *Sale of Goods Act*.

A third potential avenue to establish liability is through a nuisance claim. Nuisance is the unreasonable interference with the use and enjoyment of land in possession of another. Some examples of nuisance are: smoke damage to an insured's property caused by fire on a neighbour's property, sewage backup caused by a contactor performing work on the public sewage system, and the leaking of a neighbour's fuel tank onto the insured's property. However, not all parties can be legally pursued for nuisance. Nuisance claims against a municipality related to water and sewage damage, for example, are prohibited by s. 449 of the *Municipal Act*.

Causation
It is not enough for the insurer to claim that the third party was negligent. The insurer must establish, on a balance of probabilities, that the injury would not have occurred "*but for*" the negligence of the defendant.

In most cases, it is critical to obtain an expert opinion on the cause of the loss, as it represents an objective, detailed assessment which will guide the subrogation investigation. Some simple cases will not necessarily require an expert opinion, but most of them will.

While the legal or ultimate burden remains with the plaintiff, there are cases where the evidence will justify an inference of causation in the absence of evidence to the contrary provided by the wrongdoer. For example, it has been held that an inference of negligence against a manufacturer is compelling where the defect arose during the manufacturing process, which was controlled by the wrongdoer.

It is not always necessary to prove that a third party caused the loss in a specific way. Liability can be established if one can eliminate all reasonable possibilities other than the third party's liability. This is known as inferred liability, and can include cases where there is only one supplier and installer, where the third party had sole access to origin of the loss, or where the third party was the sole entity doing work on an element that caused the loss.

Damages

In addition to establishing legal liability, the insurer must also prove damages, including the quantum of damages being claimed, in order to be successful in their action against the wrongdoer. Depreciation of the value of the goods may reduce the quantum that is recoverable. The insured may also have to prove that there was an attempt to mitigate their damages.

Certain items will likely not be recoverable in the claim. Expert reports and investigation expenses, for example, might not be included in the quantum of damages; however, they may be recoverable as disbursements and/or in a costs award.

Once the insurer has determined the amount that can be reasonably recovered, the insurer should assess whether the quantum is worth pursing in comparison to the anticipated costs of investigating, negotiating, and litigating the claim. It may be that the damages are not significant enough to warrant the costs associated with pursuing the claim.

Early Investigation Steps

There are a number of steps an insurer should take early in an investigation to determine whether a claim is appropriate for subrogation.

While not all subrogation claims are easily established, the insurer can determine the viability of a claim by conducting a quick and effective investigation.

It is in the insurer's best interests to retain a well-respected expert as early as possible to assess the cause of the loss. However, it is not always beneficial to obtain a written report immediately. Once the expert has completed his investigation, the insurer or adjuster should obtain a verbal report as to the cause of the loss. This may identify other areas that the expert should investigate further, or may make it clear that there is no prospect of subrogation.

In the former case, the investigation can be completed without a report having already been prepared, and in the latter case, the insurer can save the cost of having such a report prepared.

It is vital that the site of the loss and any potential evidence be secured immediately. The insurer should also collect witness reports and any public investigation records, such as those from the Ministry of Labour, the TSSA, or the Office the Fire Marshal. The insurer may also consider inviting potential third parties to participate in the investigation and even conduct joint inspections for efficiency and expediency.

Where relevant evidence is in the possession of others, they should be put on notice immediately and be requested to preserve and produce the relevant evidence.

Another important step is to obtain all relevant documents from the insured, such as any contracts, leases, maintenance records, or design drawings associated with the loss.

While mitigating damages is important, all relevant evidence must be secured. This includes any pipes, plumbing fittings, sump pumps, tanks, sprinkler heads, or any other items linked to the loss. If an item failed, or worked improperly, and caused the loss, it should be preserved for testing. It is imperative that the insurer does not let repair contractors destroy the evidence.

Being aware of the best practices regarding subrogation will allow insurers to pursue all viable subrogation claims and to maintain the maximum amount of evidence to aid in any future litigation.

Adam Grant
McCague Borlack LLP
Suite 2700, The Exchange Tower
130 King Street West
Toronto, ON M5X 1C7
CANADA
(416) 862-8631
agrant@mccagueborlack.com

Liability Challengers with Over-the-Air Software Updates of Smart Devices

Seth Gausnell and Brendan Burke
Pitzer Snodgrass, P.C.

The development of the "Internet of Things" – commonly abbreviated as "IoT" – brings massive benefits, such as the ability to turn off a light without ever getting up from the couch. The shift to connect any and every object to the internet fundamentally changes the way these objects operate. Companies in the IoT economy and their insurers must understand how these changes could expose them to liability. For example, someone could hack the smart light above and gain control over, rendering its smart functionality useless. Researchers have done as much without coming within 200 feet of the light bulb.[1]

While the light example may seem harmless, the ramifications are significant given the interconnected nature of the IoT. This interconnectivity could allow hackers to spread malicious code through the air to other IoT devices, like an airborne virus on a plane. After all, if the company who sold the product can update its code wirelessly, chances are an interested third party can do the same.[2] This paper will explore the potential liability questions associated with IoT devices that can be updated over-the-air (i.e., wirelessly via the internet).

Before turning to the liability issues that accompany IoT devices, one must understand what the IoT refers to. In short, anything that connects to the internet is part of the IoT. In other words, the IoT involves extending internet connectivity beyond standard devices – such as desktops, laptops, smartphones, and tablets – to any range of traditionally "dumb" (non-internet-enabled) physical devices and everyday objects. Embedded with technology, smart devices can communicate, interact, and be updated remotely over-the-air.

Today, thanks to cheap hardware and continually-expanding wireless coverage, just about any physical object can become an IoT device. For this reason, the word "things" in the phrase Internet of Things is quite apt. For example, some of you may be wearing a smart watch, such as an Apple Watch. Others may have woken up this morning to an alarm on a smart speaker, such as an Amazon Echo. Certainly, at least one person slept through their smart speaker's alarm, but is now drinking coffee made by a smart coffee machine. These are just as few examples, but the universe of IoT devices grows each day. There are smart ovens, smart pacemakers, smart trashcans, smart belts, smart water bottles, smart buildings, smart dust, smart vacuums, and, of course, smart cars to name a few.

This year, Ericsson projects that the number of IoT devices will surpass the number of mobile phones.[3] By 2025, Intel estimates the total global worth of IoT technology could be as much as $6.2 trillion.[4] Without a doubt, growing pains will accompany this rapid growth.

[1] John Markoff, *Why Light Bulbs May be the Next Hacker Target*, New York Times (Nov. 9, 2017).
[2] *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*, HP News Advisory (July 29, 2014) (available at: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.W7F72GhKg2x).
[3] *Internet of Things Forecast*, Ericsson (last accessed Sept. 30, 2018) (available at: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast).
[4] *A Guide to The Internet of Things*, Intel (last accessed Sept. 30, 2018) (available at: https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html).

In 2015, The U.S. Federal Trade Commission ("FTC") released a report highlighting concerns about smart devices in the consumer setting, including user privacy. Smart devices are appealing because they make everyday tasks easier. However, in order to make those tasks easier, smart devices must collect large amounts of data, often including personal information from the user. The most obvious example would be smart medical devices, but all smart devices can potentially collect personal information.

Some devices, by default, are always listening, recording, and transmitting data, such as Mattel's Hello Barbie toy and Samsung's SmartTV.[5] Others, like the Google Home Mini, a smart speaker released in October 2017, only begin recording and transmitting data once they are activated by the user – or at least that's how the Home Mini was advertised. Less than two weeks before the Home Mini hit the shelves, a technology journalist discovered that the review unit he received from the Google launch event was always listening, even if he did not activate the device.[6] Apparently, a hardware flaw in the device's activation button caused his device – and many other Home Minis – to inadvertently record any conversations within earshot and transmit those recordings to Google.[7] Consequently, Google rolled out a software patch to permanently remove the functionality of the activation button in every Home Mini four days before the device was set to launch.[8] If Google can overlook such a glaring mistake, imagine what other companies with less technological experience and less money could overlook.

Furthermore, since smart devices are connected to the internet, they may provide backdoor access into a user's computer network. Thus, even if no personal information can be gleaned from the device itself, a flaw in the device may allow a malicious third-party to wreak havoc elsewhere in the user's network. At any rate, smart devices are making the personal information of consumers more vulnerable than ever. Currently, affected consumers face an uphill battle obtaining damages in court if their personal information is compromised via a smart device. The lack of consumer protection in this area prompted the Electronic Privacy Information Center to urge the Senate Commerce Committee and the Consumer Product Safety Commission to address the issue.[9]

Rather than addressing the issue of privacy in the modern context through legislation, the federal government has relied on various laws already on the books – such as the Electronic Communications Privacy Act, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act – to piecemeal the privacy rights of U.S. citizens. None of these pieces of legislation anticipated or considered a world in which everything could connect to the internet and transmit data.

[5] *Letter to Attorney General Loretta Lynch and FTC Chairwoman Edith Ramirez regarding "Always On" Devices*, Electronic Privacy Information Center ("EPIC") (July 10, 2015) (available at: https://www.epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf).
[6] *Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7*, Artem Russakovskii (Oct. 10, 2017) (available at: https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/).
[7] *Id.*
[8] *Google Home Mini touch controls behaving incorrectly*, Google Support Update (last accessed Sept. 30, 2018) (available at: https://support.google.com/googlehome/answer/7550221).
[9] Internet of Things, EPIC (last accessed Sept. 30, 2018) (available at: https://www.epic.org/privacy/internet/iot/).

The federal government also relies on the Federal Trade Commission's ("FTC") authority under Section 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful."[10] To date, the FTC has pursued several companies, including Facebook and Snapchat, for not adhering to their own privacy policies. To avoid FTC attention, companies should first employ appropriate security measures for the data they collect. The amount of security will depend on the type of data being collected. Next, companies ought to update their privacy policies to inform consumers about the nature and extent of any data the company collects. Finally, companies must comply with their privacy policies.

Since FTC actions only result in consent decrees between the FTC and the company, consumers seeking recourse for privacy violations must take their claims to court. So far, the courts have been reluctant to hear cases involving invasions of privacy, asserting that those bringing the claims do not have standing. For instance, in *Storm v. Paytime, Inc.*, a case currently before the U.S. Court of Appeals for the Third Circuit, the lower court dismissed the case because the plaintiffs did not allege that "the unidentified hacker was actually able to view, read, or otherwise understand the data it accessed."[11] Thus, according to the court, the plaintiffs did not show that the harm to their privacy interest was actual or imminent.[12] To show harm, simply showing one's personal information has been accessed does not suffice; the plaintiffs must show that their data was accessed and that they have been injured or will be imminently. Though this may be easy in cases involving identity fraud, others will prove more difficult. Accordingly, absent action by Congress or at the local level, U.S. citizens will have difficulty pursuing violation of privacy claims except in the most obvious of cases.

In addition to privacy concerns, the FTC report also pointed out novel risks of physical harm introduced by smart devices. For instance, "one participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine."[13] Another participant explained how he was able hack a smart car so that he could control the engine and braking without ever touching the car.[14]

These examples and the privacy concerns above raise several questions. What is the reasonable safety expectation for a smart device? Does the manufacturer have a duty to roll out updates to keep products safe for the entirety of their life span? Do consumers have a duty to keep their products up-to-date? These are the questions courts will ask when apportioning fault. Plaintiffs who fail to update when prompted to do so may assume some liability if the update could have prevented the harm. This becomes especially true if the company that sold the product informs the consumer about the importance of updating the device.

The questions only get pricklier after something goes wrong. Consider a semi-truck accident. To determine liability, the cause of the accident must be determined. With a "dumb" truck the possibilities were limited – the driver, the truck manufacturer, the brake manufacturer, etc. With an autonomous self-driving truck, the cause could be an obscure line of code. Perhaps a glitch in the software caused the truck to misbehave; perhaps a factory-set default password allowed it to be

[10] 15 U.S.C. Sec. 45(a)(1).
[11] *Storm v. Paytime, Inc.*, 90 F.Supp.3d 359, 368 (M.D. Pa. 2015)
[12] *Id.*
[13] *Internet of Things Privacy & Security in a Connected World*, FTC Staff Report (Jan. 2015 (available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf).
[14] *Id.*

hacked; perhaps the truck acted in accordance with its programming, but with disastrous results. As mentioned above, whether the device was up-to-date hangs in the background of all of this. These questions only become more complex as artificial intelligence continues to work its way into smart devices, further automating decision-making in smart devices.

To address some of these issues, the Center for Democracy & Technology calls for a sea change in software development practices to identify and remove bugs in code.[15] Unfortunately, debugging efforts are unlikely to ever reach perfection. Even if they did, the possibility remains that a malicious third-party could find an exploit in the code. Eventually, something will go wrong and somebody will have to pay.

Part of the process of figuring out liability exposure will involve developing a claim history. Gail McGiffin, the leader of underwriting, product, policy, and billing solutions at EY, explains that with "more and more claim activity, claim adjudication, claim litigation," we begin to "understand how the confluence of technologies and the modern work environment play out through claims, we learn how those losses are settled and the contribution of each technology — as well as the combination of technologies — to the root cause of loss."[16] As these claims develop, underwriters must rework policies to ensure all parties are aware of what risks they are assuming.

Another piece of the puzzle will be regulatory guidance. At some point, regulators will have to address the IoT to ensure consumers are protected. While regulating the IoT will help clarify the duties owed by various parties, any governmental action will likely be reactionary. Accordingly, businesses and insurers will need to pay close attention to how the courts approach these issues and respond appropriately. As with the approach to privacy liability, companies ought to update their terms of service for their smart devices. Namely, companies should explain that the device's software may be updated over-the-air from time to time and warn of the potential dangers associated with failing to update. This puts the consumer on notice, something courts will likely consider if a product with outdated software malfunctions and results in harm.

IoT technology is already changing the way the world works. Along with these changes come potential shifts in liability, particularly in devices that can update over-the-air. Beyond traditional products liability issues, over-the-air capability introduces a new threat – a cyber threat. Businesses involved in the IoT economy must talk with their insurers to ensure they have proper coverage. Insurers must anticipate and attempt to understand how the courts approach IoT issues and rework their policies accordingly. Many questions remain unanswered, but IoT companies need to be thinking about them.

Seth G. Gausnell
Pitzer Snodgrass, P.C.
100 South Fourth Street, Suite 400
Saint Louis, MO 63102-1821
(314) 335-1320
gausnell@pspclaw.com

[15] *When IoT Kills: Preparing for Digital Products Liability*, Benjamin C. Dean, Center for Democracy & Technology (April 16, 2018) (available at: https://cdt.org/blog/when-iot-kills-preparing-for-digital-products-liability/).
[16] *Artificial Intelligence Ties Liability in Knots*, Michell Kerr, Risk & Insurance (April 7, 2017), (available at: http://riskandinsurance.com/artificial-intelligence-ties-liability-knots/).

The Determination and Apportionment of Liability for IoT Products

Al De La Cruz
Manning & Kass Ellrod, Ramirez, Trester LLP

What Is the Internet of Things?

The term "Internet" is short hand for the global system of interconnected computer networks that allow the computers to communicate worldwide. It's ubiquity in human affairs is about to become secondary in size to the expanding Internet of Things (IoT). The IoT is the global universe of devices that are arguably able to communicate with each other over the traditional internet. "Though there is no specific definition of IoT, the concept focuses on how computers, sensors, and objects interact with each other and collect information relating to their surroundings."1

The IoT has been identified as the next and largest wave of the Internet. Various estimates suggest that there are currently far more IoT devices in use than cell phones worldwide. As of 2009, the number of IoT devices outnumbered people on the earth. By 2020 it is estimated that the IoT will be comprised of 50 billion devices.2 These are estimates for all types of connected devices, not just consumer market devices.

The revenue stream in the next five years from the IoT is expected to exceed $300 billion. The lure of such a lucrative revenue stream is a problem in an environment where "first to market" typically defines winners and losers in the tech race to market share.

This "first to market" concept is a driving reason why software is released before completion of full and detailed testing for reliability and security.3 Such a methodology stands in significant contrast to traditional manufacturing processes. Traditional manufacturing has learned the painful financial lessons of liability for defective and/or dangerous products.

One can imagine the revolt that would take place if automobiles, airplanes, or simple toaster ovens hit the marketplace with a catalog of flaws (bugs) inherent in their first iteration. The harm that would befall consumers until the less buggy, though not perfect, version 2.0 arrived would be unacceptable. Yet, software has avoided equal liability treatment in large part on "state of the art" justifications for flawed design and/or implementation.

The Harmful Impact of Predictable Product Failure

There are at least four vulnerabilities for consumers and businesses that are reasonably predictable:

- First is the most obvious software/firmware malfunction of an IoT device that could result in physical damage to property or personal injury. This could be a buggy controller in an industrial setting that leads to a worker injury.
- Second is lax or flawed security protection to a software system that allows a cyber intruder to harm the very people such devices are intended to benefit. Collisions involving autonomous vehicle with internet connected software upgrades are but one example with the potential for significant harm.
- A third vulnerability is an IoT product or server that is hacked resulting in stolen confidential personal data that is then later used by the hacker.

- A fourth is a simultaneous takeover of millions of IoT devices that are then used in denial of service attacks causing millions in loss or ransom.

The question arises, "Who is responsible for such harms?"

The Determination And Apportionment Of Liability For IoT Products

A new age adage is that there are two kinds of companies, those that have been hacked and those who do not realize they have been hacked. Given this truism, the reality of foreseeability of harm is virtually established. Foreseeability of harm has long been a threshold for attribution of product liability to the manufacturer as well as others in the stream of commerce.

With IoT devices, these traditional liability notions will be challenged. What product liability law will look like in 2020 is an unknown. Today, unfortunately, there are more questions than answers.

The question becomes, "Are consumer goods that combine hardware products and software solutions subject to traditional product liability tort law?" If so, how should liability for fault be apportioned amongst the various players (Primary manufacturer, sub- component firmware provider, software designers and 3rd party security overlays). If not, why should such software related failures enjoy such special protection?

Traditional Product Liability Expectations

Product liability "refers to a manufacturer or seller being held liable for placing a defective product into the hands of a consumer." Responsibility for a product defect that causes injury lies with all sellers of the product who are in the distribution chain. In general terms, the law requires that a product meet the ordinary expectations of the consumer. When a product has an unexpected defect or danger, the product cannot be said to meet the ordinary expectations of the consumer. Product liability claims are based on state laws and brought under negligence, strict liability, or breach of warranty theories.[4]

Product liability traditionally allocated and apportioned liability based on old world notions of product development and manufacturing. Component manufacturers could be expected to point to each other as the complete or partial cause for the malfunction or failure. However, regardless of such finger pointing, the creators of the product could not avoid liability to the end consumer.

If an IoT device malfunctions, how should the law allocate and apportion liability for damages?

Historically, in strict product liability a manufacturer was deemed legally responsible for physical harm caused by their products. However, the liability for damage was limited to physical harm. The end consumer could count on all members in the "stream of commerce"[5] to provide avenues for tort recovery for their injuries. However, with the proliferation of IoT devices, the grand question of liability apportionment, vis-a-vis the marriage of hardware and software manufacturers arises.

Previously, the failure costs for software technologies, be it inconvenient system crashes to costly hacking invasions, have seemingly been borne by the consumer, not the "stream of commerce" i.e. the manufacturers. Software license agreements limited liability as a matter of contract. Liability in

tort was expressly waived. However, as the IoT voluntarily moves away from such waivers, or is denied such protection as a matter of public policy, liability for harm will certainly be reallocated.

Apportionment Among Different Devices

Setting aside the hardware versus software distinction, how will liability be apportioned among multiple devices that contribute to harm? Imagine the circumstance where your phone has a software flaw that allows malware to infect your home lighting system due in part to the system's less than robust control. This in turn is used as a portal to other products, such as your home security, that tie into your home lighting controller. Traditional allocation in tort law would weigh the respective failures against their feasibility to avoid such failures and divide fault accordingly. It remains to be seen if such allocation will occur when the failure point is software that is protected by exculpatory language in its click through terms and conditions.

In each of these hypothetical situations, the question remains: "Who will bear the allocation of fault and the corresponding financial consequences?"

Under the established principles of strict product liability, fault flows up the chain of distribution from the retailer, up through distributors, sub component manufacturers, and ultimately to the final manufacturer. These risks are often contractually pre- defined between parts suppliers and manufacturers under the terms of supply agreements. Often those parties determine by market forces where a contractual duty to defend and indemnify against damages caused by a malfunctioning device will exist. Provided that such parties do not shirk their responsibility to the consumer, court intervention can be largely limited to enforcing these agreements for apportionment.

However, how will allocation of fault be shifted if the consumer plays a role? As IoT device complexity expands, might the consumer become a proper target for fault if it is found that the consumer failed to update security software which could have avoided the harm? Similarly, arguments for consumer liability will be hard to avoid if the consumer has clicked onto dubious sites that download malware. Consumer complicity through known security failures such as weak passwords may well give rise to manufacturer defenses.

It can reasonably be expected that consumers will continue to accept non-physical harm such as data loss as part of the price to be paid for convenience. However, increases in ransom ware, denial of service attacks, and the significant financial impact of system shutdowns, will drive the public policy arguments for broader liability against those most able to prevent such loss: manufacturers.

There has been several litigated cases involving IoT connected devices. However, instead of litigating product liability issues, the cases have turned on the issue of standing (lack of actual harm).6

Privacy Rights and Invasion as Harm in IoT Product Liability

Product liability theory has traditionally protected consumers from physical harm. Privacy rights and the corresponding invasion of such privacy due to product defects in software (and correspondingly "firmware" that incorporates software) is a novel theory of harm.

What issues of privacy will develop when litigation is brought and demands are made by potentially liable third parties to examine the device used by the consumer and download its contents? What issues of privacy will arise when information downloaded from an IoT product is stolen? What issues of privacy will exist when information collected from an IoT-connected device is sold by the IoT device manufacturer to a third party?

As an example, how are damages related to privacy issues to be compensated? What if there is a security breach and private information is obtained and even shared but there is no evidence of use? Are such breaches actionable in the absence of demonstrable harm? Damages related to privacy issues are very difficult to quantify. These types of damages, or lack thereof, also create legal questions of standing.

Assuming standing exists, how do you allocate responsibility for damages? Does legal fault lie with the criminal acts of a hacker, with the poor intended, rushed manufacturer, or with the owner who may have failed to properly secure the product (i.e., by using a weak password or by failing to timely updating the software)? If there is a software failure versus an actual defect in the product, should the maker of a product be held liable for the software failure? What if the manufacturer of the product or the software failed to include sufficient security designs? What about component part liability? Traditional product liability law holds that defective component part manufacturers can be held liable. Whether courts will extend this doctrine to this arena is still unknown.

Conclusion — A Historic Opportunity

Given the predictions regarding the number of IoT devices expected to exist near future, the volume of consumer claims will only continue to grow. Traditional product liability theories will need to be examined and re-examined against this changing technical and legal landscape. The IoT has not only changed the way we live, it will change how we think about traditional notions of product liability law. We will need courts and legislators who will move with greater alacrity to meet these challenges.

In March of 2018, LexisNexis released the first comprehensive research study to examine the insurance industry's perspective on collecting, analyzing, and using data created by the Internet of Things (IoT). The study found that while insurance carriers recognize the potential value and impact such data will have on the industry, few carriers collect IoT data, have an IoT strategy, or have dedicated resources in place to address this emerging issue.

Such reality affords a competitive advantage and opportunity for forward-thinking insurers who endeavor to learn this emerging technology. While the law governing liability will likely evolve over the next several years, investing time to stay abreast of these developments is well worth the effort.

Al De La Cruz
Manning & Kass Ellrod, Ramirez, Trester LLP
550 West C St Ste 1900
San Diego, CA 92101-3569
(619) 515-0269
amd@manningllp.com

1. Antigone Peyton, A Litigator's Guide to the Internet of Things, 22 RICH. J.L. & TECH. 9 at 1 (2016), available at http://jolt.richmond. edu/2016/04/01/a-litigators-guide-to-the-internet-of-things/

2. Dave Evans, The Internet of Things: How the Next Evolution of The Internet is Changing Everything at 3, Cisco Internet Bus. Solutions Grp. (April 2011), available at https://perma.cc/HDF9- NM6T](https://perma.cc/HDF9-NM6T

3. The Half-Truth of First-Mover Advantage, Fernando Suarez and Gianvito Lanzolla, Harvard Business Review (April 2005) https://hbr. org/2005/04/the-half-truth-of-first-mover-advantage]

4. Restatement (Third) of Torts: Product Liability §§ 1-2 (1998)

5. World-Wide Volkswagen v. Woodson 444 U.S. 286 (1980)

6. An Exploration of Strict Products Liability and the Internet of Things Benjamin C. Dean (April 2018) Center for Democracy & Technology https://cdt.org/files/2018/04/2018-04-16-IoT-Strict- Products-Liability-FNL.pdf

Smart Thermostats and Beyond:
Impact of the Internet of Things on Litigation of Product Liability Claims

Jim Tomlinson and Andrew Valela
McCague Borlack LLP

The "Internet of Things", generally referred to as the "IoT", is a concept that has become increasingly commonplace in daily life due to rapid developments in technology. The IoT deals primarily with the idea of connectedness between devices, systems, and networks. It refers to the network of "smart" devices that have the capacity to connect, communicate, and exchange data with one another via the internet. While these devices impact the way we live by creating efficiencies and making our personal lives more convenient, they are accompanied by risks that present challenges for insurers. Given that IoT devices have the capacity to communicate with each other and with third party devices, and given the various interdependencies that allow these devices to operate harmoniously, IoT products are subject to the risk of malfunctioning. They may also be vulnerable to external threats, such as software glitches and control by third party hackers. When an IoT device malfunctions without physical human intervention and causes a loss, the question of who is liable for the loss becomes pertinent. This question has implications for both product liability and product safety regimes.

Consider the simple example of a smart thermostat. Smart thermostats allow you to control the temperature of your home via your smart phone, tablet, or other internet-connected device using a mobile application. The thermostat is connected to your home Wi-Fi network, as well as your HVAC, furnace, or boiler system. The app allows you to control your thermostat even when you are not at home. For the purposes of this example, imagine that the thermostat is exposed to a software bug which causes it to turn off in the dead of winter. Alternatively, consider the scenario where your thermostat is hacked by a third party causing it to malfunction and turn off. The lack of heat inside your home causes your pipes to freeze and burst, resulting in a flood. Using this example as a point of reference, this paper will highlight some of the considerations that adjusters should address when handling claims involving IoT devices, and the challenges that legal counsel may encounter when trying to assess liability following an IoT-related loss. It will also consider how policy wordings respond to these types of losses, and current legislative initiatives that are working to address the risks associated with IoT products.

I. Retaining the Right Investigators

Following a loss, one of the first things that adjusters do is retain investigators. Investigators play a crucial role as they assist in determining who is responsible for the loss. This assists legal counsel in determining which parties to name when commencing an action. The right investigators will need to be retained given that IoT-related losses are more complicated than other types of losses. This may prove to be difficult however since the evidence involved in claims involving IoT devices will likely be more complex. Investigators will need to consider the manner in which the IoT device interacted or communicated with other connected devices prior to the loss, and the roles of the various devices in facilitating the proper functioning of the IoT device. Investigators will also need to obtain copies of the contracts between software companies and IoT product manufacturers to see how risks are allocated and to determine who has responsibility for performing certain functions. In the context of our hypothetical example, it will be necessary for the investigator to analyze the interaction and

interrelationships between the thermostat, mobile application, Wi-Fi network, and other components to which the device is connected in order to provide a preliminary assessment with respect to the cause of the loss.

II. Who to Name as a Party to the Action

When planning to commence a subrogated action on behalf of an insurer, counsel faces the initial challenge of determining which parties to name in the proceeding. Counsel will typically consider the cause of the loss, followed by those who are responsible for the loss. This is why it is important to have an investigator attend the scene shortly after the loss occurs. In typical cases involving floods or water damage, liability is dependent on the cause or source of the water escape. In cases involving IoT devices, it becomes much more difficult to pinpoint the exact cause of the loss. This is a result of the interconnectedness between the various IoT devices, applications, and third party products which allow the connected devices to operate. It is also due to the fact that IoT devices rely heavily on applications in order to function, and often there is more than one application involved in connecting IoT devices to one another. If these connections or applications malfunction, there is a risk that the product could fail. For these reasons, first party insurers commencing subrogated actions stemming from IoT-related losses must consider additional parties to add to the action who may not have been considered necessary parties in the past (for example, intermediary app developers). Similarly, counsel defending an insured from an IoT-related lawsuit must look to additional parties to bring into the action via third party claims. Using our smart thermostat example, counsel should consider including the following parties in the lawsuit: the manufacturer of the thermostat, the retailer who sold the product to the insured, the installer, the intermediary app developers, and the manufacturers or retailers of any connected devices or components.

III. New Types of Experts

If there is a problem in pinpointing the exact cause of the loss, this will have implications in terms of retaining the appropriate experts. Counsel planning to commence a subrogated action will need to involve different classes of experts when dealing with IoT-related losses. This may not necessarily be an electrical engineer. Insurers may need to retain IT experts/analysts who can interpret the different kinds of data and evidence produced by IoT devices, which electrical engineers, for example, may not be trained to do. Potential experts might include individuals with technical expertise in computer engineering, software engineering, and the implementation, monitoring, or maintenance of IT systems. However, an issue that arises is whether these new types of experts will have the requisite knowledge and expertise to address the cause of a loss, and whether they can withstand cross-examination pertaining to their qualifications and analytical techniques.

An analogous issue was considered by the U.S. District Court for the District of Maryland in *American Strategic Insurance Corp. v Scope Services, Inc.*[1] The case involved the installation of a smart meter used to monitor energy usage in a home, which subsequently failed and caused extensive damage to the property. The defendant argued that the plaintiff's expert was not qualified to act as an expert witness because he did not have experience installing smart meters, and was therefore unable to provide testimony regarding the applicable standard of care. The Court held that plaintiff's expert witness was not permitted to opine on the standard of care for the installation of a smart meter, notwithstanding that he did qualify to testify as an expert in electric meter installation.[2] The Court stated that the expert's testimony on the standard of care amounted to "little more than his

[1] *American Strategic Insurance Corp. v Scope Services, Inc.*, 2017 US Dist LEXIS 149789 (D Md).
[2] *Ibid.*

personal views on the proper method of smart meter installation."[3] Given this decision, adjusters and counsel will need to be increasingly mindful of how the opinions of the experts they retain will hold up in a courtroom setting.

IV. Implications for Insurance Policies

With the number of IoT devices estimated to reach approximately 30 billion by 2020,[4] one has to wonder how insurers will respond when an IoT device fails and whether they will adjust their policy wordings to eliminate gaps in coverage. For businesses, Commercial General Liability ("CGL") Policies will typically provide coverage when an IoT product fails and causes a loss. However, the implications for businesses may be significant. For example, IoT device failures could lead to business interruption losses, such as the closure of a manufacturing plant and lost revenues. For these reasons, businesses should consider obtaining business interruption insurance to help alleviate the repercussions of an IoT product failure. Contingent business interruption ("CBI") insurance may also be necessary, as it provides protection for lost revenues and additional expenses resulting from interruptions to the businesses of third party suppliers and key customers. Brokers will need to be aware of these products when approached by businesses looking for insurance coverage.

For homeowners, one issue that arises is how traditional insurance policies will respond to losses resulting from the failure of an IoT device. Redesigning policies to allow for coverage when this occurs would certainly be beneficial for insureds. However, insurers will not want policies so broadly worded that they will be required to respond to every loss involving an IoT device. Careful consideration of these issues will be required as insurance companies continue to grapple with the risks posed by the IoT. For example, an important question pertaining to coverage arises when an IoT device is hacked by a third party. Where a hacker assumes control over an IoT device (such as a smart thermostat) and intentionally causes a loss, one cannot say that the product has "failed" in the traditional sense. In their policies, insurers will need to draw a distinction between the deliberate actions of third party hackers and the unprovoked failure or malfunctioning of an IoT device.

Furthermore, IoT product manufacturers will need to obtain insurance coverage to respond to lawsuits involving the alleged failure of their products. Insurers are now beginning to provide increased protection to IoT product manufacturers for risks that are typically not covered by traditional insurance policies. Included in this protection is liability coverage for errors and omissions stemming from the defective design and manufacture of IoT devices.[5] These policies extend to defend insureds if they get sued as a result of an IoT product failure. Insurers may also offer coverage for cyber extortion threats involving IoT products.[6] Companies involved in the manufacture of IoT devices will need to consider these products in order to obtain coverage for risks that are generally not insured under traditional policies. Similarly, as technology continues to advance, insurers will need to develop additional products in order to respond to the evolving needs of IoT product manufacturers. However, insurers will not want to make their policy wordings overly prescriptive so as to name every potential peril that could result in loss or damage. This is due to the

[3] *Ibid.*

[4] "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)", *Statista*, online: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.

[5] "Enhanced Coverage for Internet of Things Product Manufacturers" (2017), *Marsh*, online: <https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/IoT-insurance-product-FS%20FINAL.pdf>.

[6] *Ibid.*

fact that advancements in technology make it difficult to determine what types of perils will need to be covered in the future.

V. Current Regulatory Initiatives

At a potential trial involving the failure of an IoT device, there will be an issue regarding what types of evidence will need to be adduced in order to prove that the standard of care was breached. This is due to the fact that product liability regimes were not designed to take into account the risks associated with IoT devices. While some nations are beginning to develop standards concerning IoT devices, there are currently no universally acceptable product safety standards for IoT devices.

In the United States, the Consumer Product Safety Commission ("CPSC") is taking an active role in regulatory initiatives involving IoT products. On March 27, 2018, the CPSC announced that it would be holding a public hearing "to receive information from all interested parties about potential safety issues and hazards associated with internet-connected consumer products."[7] The hearing took place on May 16, 2018.[8] Following the hearing, the CPSC gave interested parties the opportunity to submit written comments through to June 15, 2018. In their March 2018 announcement, the CPSC noted that the product safety challenges of IoT products appear to fall into two main categories: 1) prevention or elimination of hazardous conditions designed into products intentionally or without sufficient consideration; and 2) preventing and addressing "incidents of hazardization."[9] In addition, the notice provided examples of hazards created by IoT devices, including remote operation, unexpected operating conditions, loss of a safety function, and hazards created from unintended product features.[10] Using the information obtained during the hearing and from the written submissions, the CPSC is working to develop voluntary standards related to the IoT. Adjusters and legal counsel will need to closely follow the efforts of the CPSC to see how this initiative unfolds.

It should also be noted that the United States Federal Trade Commission ("FTC") has jurisdiction with respect to cases involving IoT products. The focus of the FTC is on the privacy and security risks associated with the IoT. The jurisdiction of the FTC also extends to design flaws pertaining to IoT products if they lead to security breaches or unauthorized access to data, as evidenced in the FTC's complaint against ASUSTeK Computer, Inc.[11] In that case, the FTC alleged that ASUSTeK failed to take reasonable steps to secure the software for its routers, which resulted in a security breach.[12] A settlement order was reached between the FTC and ASUSTeK, which required the tech company to establish and maintain a comprehensive security program subject to independent audits for the next 20 years.[13]

[7] U.S. Consumer Product Safety Commission, "Internet of Things and Consumer Product Hazards" (March 27, 2018), *Federal Register*, online: <https://www.federalregister.gov/d/2018-06067>.
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*
[11] Federal Trade Commission, Press Release, "ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk" (February 23, 2016), online: <https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put>.
[12] Federal Trade Commission, Press Release, "FTC Approves Final Order in ASUS Privacy Case" (July 28, 2016), online: <https://www.ftc.gov/news-events/press-releases/2016/07/ftc-approves-final-order-asus-privacy-case>.
[13] *Ibid.*

In the Canadian context, the *Canada Consumer Product Safety Act* ("*CCPSA*" or the "Act")[14] establishes a regulatory regime for consumer products. Administered by Health Canada, the stated purpose of the *CCPSA* is to "protect the public by addressing or preventing dangers to human health or safety that are posed by consumer products in Canada, including those that circulate within Canada and those that are imported."[15] Given that the *CCPSA* came into force in 2011, the frameworks contained within the Act are fairly modern. The key provisions of the Act relate to mandatory reporting of product safety incidents and product defects, preparation and maintenance of records, obtaining product safety information (such as tests and studies), and prohibiting unreasonably dangerous products.[16] From the Canadian perspective, there is an expectation that these frameworks can deal with safety issues stemming from IoT products. However, given the fact that the IoT is still in its early stages, it remains to be seen whether the *CCPSA* can cope with recent developments in technology. While there have not yet been any reported incidents or defects involving IoT products pursuant to the Act's mandatory reporting requirements, this is not necessarily indicative. For example, an IT company was recently asked to hack into an Oakville, Ontario, family's smart home for the purpose of testing its security.[17] The "ethical" hackers were able to do so in a matter of hours, giving them the ability to unlock the front door of the home, manipulate the lights and thermostat, and obtain control over security cameras.[18] This example illustrates the potential product safety concerns that the *CCPSA* may need to deal with in the future.

The *CCPSA* is not the only Canadian initiative directed at product safety as it relates to the IoT. Health Canada is closely following the efforts of the CPSC. It also participated in the CPSC's public hearing that was held in May of 2018. With the increasing prevalence of IoT products, Health Canada hopes to work with the CPSC in order to identify gaps in existing regulatory frameworks and to fill those gaps through additional regulatory efforts. Collaboration between Health Canada and the CPSC to develop a set of product safety standards pertaining to IoT devices would greatly benefit North American consumers. Health Canada and the CPSC have collaborated on consumer product safety in the past. For example, both entities recently ratified a trilateral memorandum of understanding ("MOU") with the Mexican Office of the Federal Prosecutor for the Consumer ("PROFECO").[19] The objective of the MOU is to facilitate cooperation and coordination between the three nations in relation to product safety.[20] With these initiatives, Canada may be one step closer to the development of safety standards specific to IoT products.

[14] *Canada Consumer Product Safety Act*, SC 2010, c 21.
[15] *Ibid*, s. 3.
[16] "Meeting Canada Consumer Product Safety Act Requirements" (March 13, 2018), *Government of Canada*, online: <https://www.canada.ca/en/health-canada/services/consumer-product-safety/legislation-guidelines/acts-regulations/canada-consumer-product-safety-act.html>.
[17] Luke Denne, Greg Sadler & Makda Ghebreslassie, "We hired ethical hackers to hack into a family's smart home – here's how it turned out", *CBC* (September 28, 2018), online: <https://www.cbc.ca/news/technology/smart-home-hack-marketplace-1.4837963>.
[18] *Ibid.*
[19] U.S. Consumer Product Safety Commission, Press Release, "North America Product Safety Regulators Agree to Increase Cooperation on Consumer Product Safety; Trilateral MOU Signed at Annual Meeting of Multi-Stakeholder Association" (February 22, 2018), online: <https://www.cpsc.gov/content/north-america-product-safety-regulators-agree-to-increase-cooperation-on-consumer-product>.
[20] U.S. Consumer Product Safety Commission, Health Canada, Office of the Federal Prosecutor for the Consumer, "Memorandum of Understanding" (February 22, 2018), online: < https://www.cpsc.gov/s3fs-public/Signed_Trilateral_MOU_English_2018.pdf>.

VI. Final Thoughts

There is no doubt that the IoT will impact the way in which product liability claims are litigated. The number of IoT products available to the public is rapidly growing, but in many instances there are inadequate safety measures in place to prevent the malfunctioning and failure of these products. The absence of such safety measures creates challenges not only for adjusters and counsel when faced will IoT-related losses, but also end consumers. Moreover, the fact that IoT products are often similar in design raises additional issues, given that hackers are able to exploit common vulnerabilities across a wide array of devices.

In the future, insurers may need to redesign their policies to adapt to the new risks posed by IoT products. In addition, IoT product manufacturers will need to carefully consider the legal issues involved in bringing their products to market. Manufacturers should especially examine these issues when drafting contracts with suppliers, software developers, and app developers. Without express language in the contracts, there will be uncertainty as to which party will assume responsibility for a product failure. IoT manufacturers will also need to evaluate the safety features of connecting products and applications prior to entering into any contracts. They may also want to obtain commitments from suppliers and developers to keep firmware and software up to date in order to reduce the risks of product failure.

Currently, there are no safety standards that take into account the unique vulnerabilities of IoT products. This could change in the future, given the increasing number of IoT products and the growing threat of exposure to third party hackers. The initiatives undertaken by the CPSC appear to be leading the way in the development of product safety standards for IoT devices. Therefore, adjusters and counsel will need to be mindful of emerging regulatory trends moving forward, and will have to closely follow how courts are resolving cases involving IoT product failures.

Jim Tomlinson
McCague Borlack LLP
Suite 2700, The Exchange Tower
130 King Street West
Toronto, ON M5X 1C7 Canada
(416) 860-0001
jtomlinson@mccagueborlack.com

Issues Arising from Legalization of Medicinal and Recreational Cannabis

Thomas A. Kendrick
Norman, Wood, Kendrick & Turner

Part 1: Medicinal Marijuana: Use and Misuse

Introduction

In 1996, the State of California passed the first laws approving the medical use of marijuana. As of January 22, 2018, similar laws have been enacted in 30 additional states, bringing the total number of state allowing use of medical marijuana to 31. The District of Columbia and the territories of Guam and Puerto Rico have also enacted similar legislature. Fifteen additional states have approved the use of "low THC, high cannabidiol (CBD)" products in limited situations. Although these programs are not counted as comprehensive medical marijuana programs, 46 of the 50 United States now allow some use of cannabis for medical reasons, creating interesting conflicts between federal law and state law, as well as scientific and social issues.

Tetrahydrocannabinol (THC) and Cannabidiol (CBD)

Tetrahydrocannabinol (THC) and cannabidiol (CBD) at two natural compounds found in *Cannabis* plants. THC is the main psychoactive compound in marijuana that produces the high. CBD is not psychoactive, despite having the same molecular structure as THC. THC binds with the cannabinoid receptors in the brain, producing a sense of euphoria or high. CBD binds weakly or not at all to the brain receptors and can even inhibit the binding of THC to the brain receptors.

State and Federal Conflicts

Until September 2018, marijuana remained classified as a Schedule I substance under the Controlled Substances Act as a substance having a high potential for dependency and no accepted medical use. The United States Drug Enforcement Administration has now moved drugs with less than 0.1% THC content to Schedule V, as long as the drugs have been approved by the U.S. Food and Drug Administration (FDA). This change was prompted by the FDA's approval of the drug Epidolex, a drug intended to be used in rare forms of epilepsy. Other than drugs containing small amounts of THC or CBD that have been approved by the FDA, distribution of marijuana is still a federal offense. As public opinion has increased toward the acceptance of medical use of marijuana, the U.S. Department of Justice announced in 2009 a change in the enforcement policy, deferring enforcement of marijuana violations to the states. However, in January 2018, Attorney General Sessions rescinded the memorandum, allowing federal prosecutors to decide how to prioritize the enforcement of federal marijuana laws. Attorney General Sessions *Marijuana Enforcement Memoranda* directs U.S. attorneys to "weigh considerations, including federal law enforcement priorities set by the Attorney General, the seriousness of the crime, the deterrent effect of criminal prosecution, and the cumulative impact of a particular crimes on the community." See (*Marijuana Enforcement Memorandum*, https://www.justice.gov/opa/pr/justice-department-issues-memo-marijuana-enforcement)

The conflict between state and federal law over marijuana enforcement has created issues for physicians who cannot prescribe or dispense marijuana for medical use without violating federal drug enforcement laws. Since physicians cannot prescribe medical marijuana, but can only certify a

patient as having an appropriate diagnosis to allow the patient to obtain registration, problems have developed concerning medical management. Since physicians cannot dispense, the management of access to medical marijuana and management of dosing falls on the dispensary, rather than a physician or pharmacist. Common policy questions include how to regulate the recommendations of medical marijuana, dispensing of medical marijuana, and the registration of approved patients. Medical marijuana producers for dispensaries are often classified as "caregivers" subject to state regulations concerning the amount of product produced and dispensed per patient.

Research Supporting the Use of Medical Marijuana

The efficacy of the use of marijuana as medicine has been a matter of much recent debate as policy makers and scientists grapple with the question of whether the expansion of the use of medical marijuana is the result of scientific-based research or is driven by public opinion? Two studies were released in 2017 which looked at the scientific research behind the medical use of marijuana. In January 2017, the National Academies of Sciences, Engineering and Medicine (NASEM) published a comprehensive report titled, "The Health Effects of Cannabis and Cannabinoids, The Current State of Evidence and Recommendations for Research." The NASEM convened an hoc expert committee to develop a comprehensive, in-depth review of the most recent evidence regarding health effects of using cannabis and cannabis-derived products. The Committee presented nearly 100 different research conclusions, organizing these into categories where the evidence is conclusive, substantial, moderate, limited, and no/insufficient evidence. The Committee concluded that medical marijuana is effective in certain instances, not effective in others, and pose certain risks, including mental health issues. The Committee made the following recommendations to prioritize research approaches and objectives:

1. "Address current research gaps, highlighting the need for a national cannabis research agenda that includes clinical and observational research, health policy and health economics research, and public health and public safety research";
2. "Identify actionable strategies to improve research quality and promote the development of research standards and benchmarks";
3. "Highlight the potential for improvements in data collection efforts and the enhancement of surveillance capacity"; and
4. "Propose strategies for addressing the current barriers to the advancement of the cannabis research agenda."

See the Committee's Recommendations, *The Health Effects of Cannabis and Cannabinoids* The Current State of Evidence and Recommendations for Research, the National Academies of Sciences Engineering Medicine, January 2017.

The Committee of the NASEM found conclusive or substantial evidence that cannabis or cannabinoids are effective for the treatment of chronic pain in adults, use as an anti-emetic in the treatment of chemotherapy-induced nausea and vomiting, and for improving patient-reported multiple sclerosis spasticity symptoms. The Committee addressed many other diseases, reaching almost 100 conclusions concerning the health effects of cannabis and cannabinoids.

A second study published later in 2017 reviewed the publication of research between January 2009 and January 2017. This study concluded: "The public perception of the efficacy, tolerability, and safety of cannabis-based medicine in pain management and palliative medicine conflicts with the

findings of systematic reviews and prospective observational studies conducted to the standards of evidence-based medicine." See *Cannabinoids and Pain Management and Palliative Medicine, an Overview of the Systematic Reviews and Prospective Observational Studies*; Winfred Hauser, Mary-Ann Fitzcharles, Lukas Radbruch, and Frank Petzke, Dtsch Arztebl Int 2017; 114:627-34.

Part 2: Legalized Recreational Use of Marijuana: Liabilities and Legal Issues for Employers, Insurers, and Insureds

Recreational use of marijuana has now been approved in eight states, including Colorado, Nevada, California, Oregon, Washington, Alaska, Massachusetts, and Maine. While regulatory issues concerning the growing and dispensing of recreational marijuana are not fully implemented, employers, employees, insurers, and insureds are facing new legal challenges regarding the use of recreational marijuana.

Employee Drug Testing

The legalization of marijuana for recreational and medicinal use has created a number of employment issues for employers. In the late 1990s, many employers developed zero-tolerance policies regarding drug use. Employees were often required to submit urine specimens for pre-employment testing. Thereafter, the employees would be administered random drug tests. If an employee tested positive for a controlled substance, the employee would have an opportunity to explain to a medical review officer whether there was a reasonable explanation for the positive test. If there was no such explanation, then the urine drug screen would be reported to the employer as positive, subjecting the employee to disciplinary action, including termination. With the legalization of the use of marijuana for recreational and medicinal purposes, many employers have revised their drug testing policies. Some employers have abandoned drug testing all together, while others have limited testing to positions involving significant safety risks. While private employers have been able to conduct drug tests without the same constitutional concerns faced by public employers, private employers are now finding that state regulations that permit the recreational and medicinal use of marijuana create obstacles to their traditional drug testing programs.

Private Employers

A Connecticut Federal Court recently concluded that a prospective employee, who applied for a job in a nursing home, was wrongfully denied employment upon testing positive for cannabinoids. The job applicant was a registered and qualified user of medical marijuana. Her pre-employment test was positive for THC, and the nursing home rescinded her job offer, sighting a zero-tolerance/anti-drug policy. In the case of *Noffsing v. SSC Niantic Operating Company, LLC,* the applicant challenged the fact that her job offer was rescinded. The nursing home cited its zero-tolerance policy, as well as the fact that marijuana is illegal under federal law. However, the United States District Court in Connecticut concluded that Connecticut's Palliative Use of Marijuana Act (PUMA) contained an anti-discrimination provision that was not preempted by federal law. Although the Court noted that the Connecticut law does not limit an employer's ability to prohibit the use of intoxicating substances during work hours, it does protect an applicant, who may use marijuana outside of work hours and in the absence of any evidence of influence during work hours, from discrimination in employment. For private employers in states that now permit recreational and medicinal use of marijuana, employers should re-evaluate their drug testing policies to be certain they do not conflict with the state regulations.

One challenge facing employers is the question of whether an employee is under the influence of an intoxicating substance while on the job. A positive test for cannabinoids does not necessarily indicate impairment. Thus, the determination of whether an employee is impaired usually falls on the common signs of impairment, such as red eyes, increased appetite, poor coordination, erratic behavior, tremors, impaired motor skills, and the smell of marijuana. States are developing criteria for testing to determine appropriate levels of THC that would indicate impairment. Levels that are presumptive for legal intoxication are anticipated in the future.

Public employers

The rules concerning drug testing for public employers are different in that public employers are subject to the provisions of the Fourth Amendment protections offered by the United States Constitution. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." United States Constitution, Amendment IV. Thus, public employers, such as states, counties, municipalities, and school boards, have been limited in the ability to conduct employment drug testing. An individual's privacy expectations must be weighed against the government's interest in testing. The United States Supreme Court has never endorsed a broad, across the board, suspicion less drug testing of all public employees, and it is doubtful that the United States Supreme Court will ever do so.

Many cases throughout the circuits have addressed positions subject to suspicion less testing, including paramedics/EMTs, healthcare providers, CDL drivers, regular drivers, positions that work with drugs or controlled substances, positions requiring employees to carry a firearm, police officers, firefighters, heavy equipment operators, school bus mechanics, positions requiring close work with children, and positions which work with classified or highly sensitive criminal information. Thus, where there is a compelling governmental interest in issues of safety or security, employees may be tested in pre-employment or random post-employment drug testing programs. However, as in the Connecticut case cited above, any drug testing program must comply with the state regulatory requirements that may be enacted through state legislation permitting recreational or medicinal drug use.

Liability Issues for Insurers/Insured

The legalization of marijuana for recreational and medicinal use has resulted in a 3% increase in automobile accidents. Liability issues for insurers and insureds are expected to increase as recreational use of marijuana increases. States must develop criteria for levels of THC that will support a presumption of impairment, similar to blood alcohol levels. On-the-job injuries are also likely to increase, implicating issues for workman compensation insurers.

Legal sales of marijuana grew by 30% in 2016. Cannabis related businesses are facing many new risks and obstacles in the insurance market. As cannabis related businesses grow, the demand for insurance policies insuring against risks of employee theft, general liability, and product liability will increase. The cannabis related businesses will face the same risks as other agricultural and manufacturing businesses face, including work place injuries, damage to property, crop failure, and product liability and safety recalls. State insurance regulators are faced with new challenges as they seek to understand the needs and gaps as the insurance industry evolves to provide protection for new risks.

Conclusion

While scientific research continues, the current research supports the use of medical marijuana based on specific patient needs, but it is not a natural panacea. Additional research is required. In the meantime, the state legislatures and courts must deal with potential issues arising from the conflict of laws, interstate commerce, privacy considerations, and discrimination claims. The scientific, legal, and social implications are far from settled.

As with any new business line, the opportunities are many, but the risks will be challenging. Employers, insurers and state negotiators are faced with many new challenges in a rapidly expanding market.

Thomas A. Kendrick
Norman, Wood, Kendrick & Turner
Ridge Park Place Ste 3000
1130 22nd St S
Birmingham, AL 35205
(205) 259-1032
tkendrick@nwkt.com

The Current State of the Opioid Crisis in the United States and Opioid Litigation

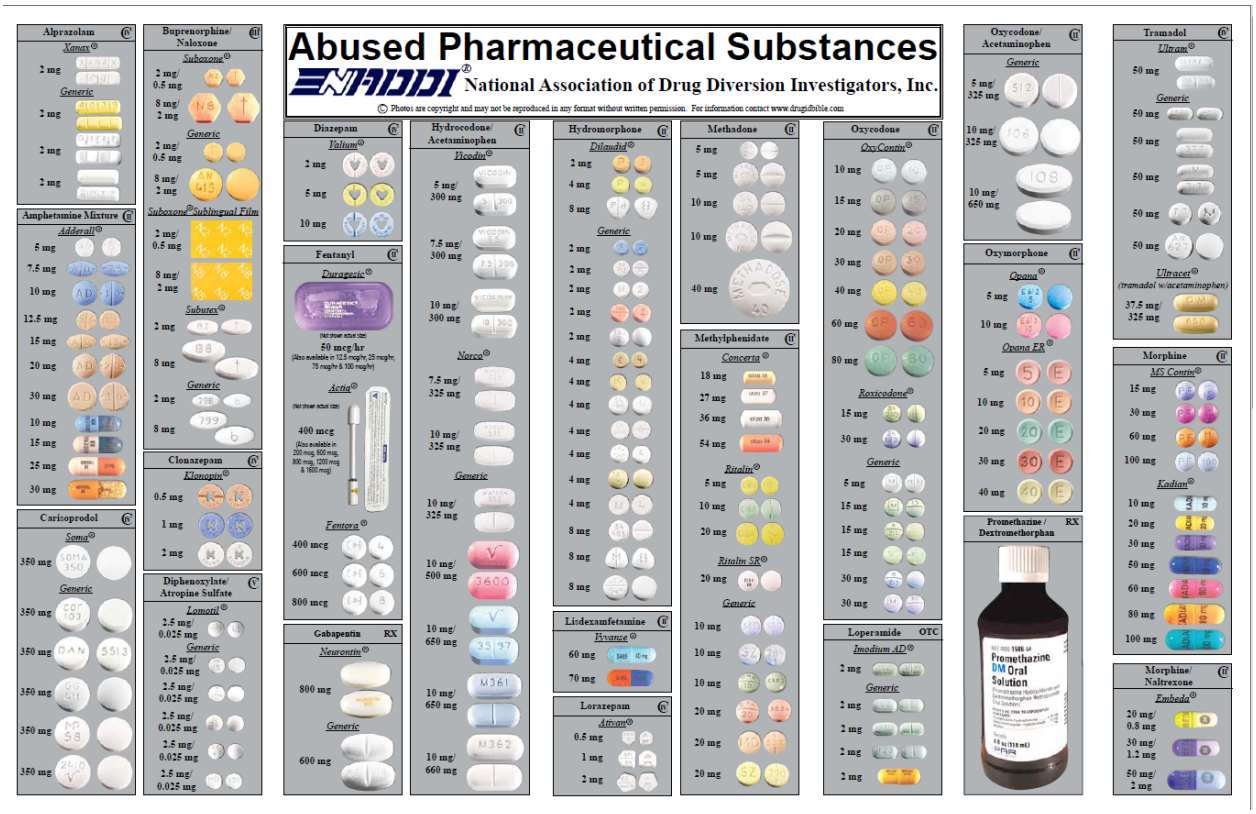
Thomas R. Maeglin & Glenn A. Jacobson
Abrams, Gorelick, Friedman & Jacobson, LLP

Introduction

The United States of America is experiencing a widespread and prolonged crisis of opioid abuse, drug addiction and overdoses and death. Unlike other drug abuse crisis of the past, the opioid crisis knows no racial, socioeconomic, gender or age boundaries. It is claimed to have its genesis in the manufacture and distribution of legal but controlled pharmaceuticals that has spawned a wave of litigation against drug manufacturers, distributors, and pharmacies and in some cases individual shareholders, officers and executives of these companies. This paper will provide a brief introduction to the crisis, the current status of the litigations and address some issues regarding insurance coverage for the claims that are being addressed by American courts.

A. What are Opioids

The Centers for Disease Control and Prevention describe opioids as "[n]atural or synthetic chemicals that interact with opioid receptors on nerve cells in the body and brain, and reduce the intensity of pain signals and feelings of pain." (See Centers for Disease Control and Prevention, "Commonly Used Terms", found at https://www.cdc.gov/drugoverdose/ opioids/terms.html.) Opioids are a class of drugs that include many well-known prescription pain medications such as codeine, hydrocodone, morphine and oxycodone, as well as the illegal drug heroin and synthetic opioids such as fentanyl. Prescription opioids, or opioid analgesics, are used to treat moderate to severe pain. Opioids can be categorized as natural opioid analgesics (including morphine and codeine); semi-synthetic opioid analgesics (including oxycodone, hydrocodone, hydromorphone, and oxymorphone); or as synthetic opioid analgesics other than methadone (including tramadol and fentanyl).



Source: National Association of Drug Diversion Investigators, Inc., "Abused Pharmaceutical Substances", 09/2018.

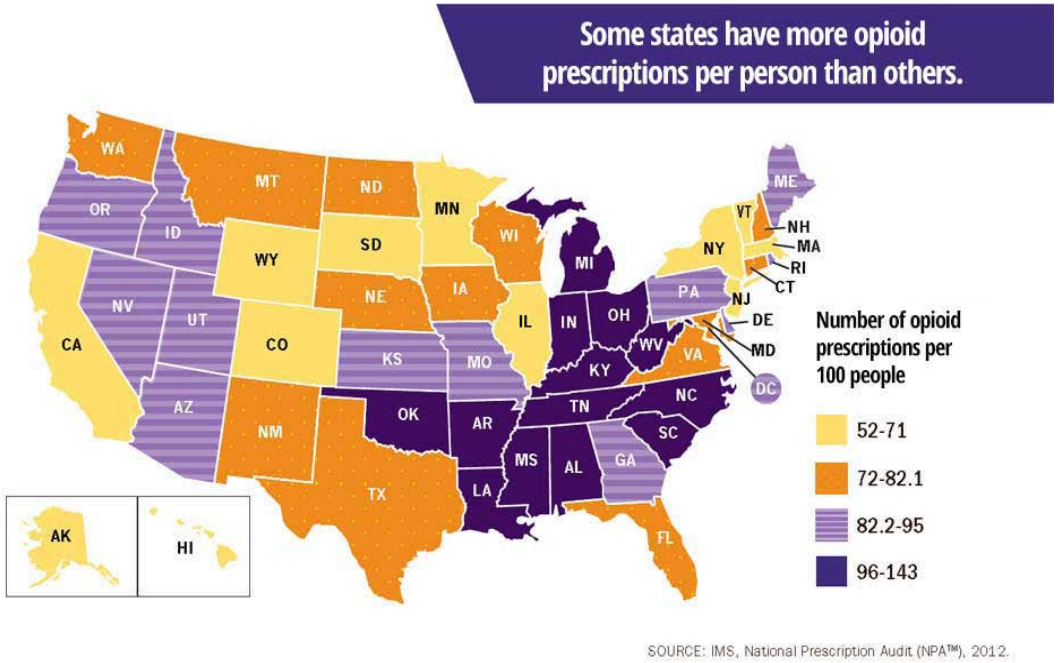
Opioid analgesics can also be classified according to the speed by which they are absorbed by the body and duration of their effects. The original opioid products were immediate-release opioids which were relatively faster-acting medications with a shorter duration of pain-relieving action. Extended-release/long-acting (ER/LA) opioids were developed in the 1990s, giving slower-acting effects with a longer duration of pain-relieving action.

Related to and an important part of the Opioid Crisis are certain non-medical opioids. Heroin is an illegal, highly addictive opioid drug processed from morphine a natural substance taken from the seed pod of the opium poppy plant. Methadone, the well-known treatment for heroin addiction, is a synthetic opioid. Similarly, there are legal and illegal varieties of fentanyl. Pharmaceutical fentanyl is a powerful synthetic opioid pain medication that is similar to morphine. A schedule II drug, it is 50 to 100 times more potent than morphine and prescribed to treat patients with severe pain. However, illegally made fentanyl has become widely available in illegal drug markets due to its heroin-like effect and much higher potency, and it is often mixed with heroin and/or cocaine as a combination product. See id. CDCP. The combination of fentanyl with these other drugs is directly related to the increase in overdose deaths.

People have used products produced from the opium poppy for millennia. Opioids have been in use since the discovery of morphine in the early 1800's. In the United States, through the 1980's, opioid analgesics were largely used for treatment of severe pain, such as in patients suffering from malignant cancer. Concerns about addiction, as well as the limited duration and declining benefits of opioid products limited their medical use. Opioids developed in the 1990s were intended to act

on a slower, more long-lasting basis to give relief to sufferers of less severe but nonetheless chronic pain, with a lower risk of abuse and addiction. Today, the CDCP still advises that "Opioid pain medications are generally safe when taken for a short time and as prescribed by a doctor, but because they produce euphoria in addition to pain relief, they can be misused." (See id., CDCP).

The companies engaged in the manufacture, distribution and dispensing of opioids include many well-known American and international companies, such as Purdue Pharma, Cephalon, Teva Pharmaceuticals, Endo Pharmaceuticals, Janssen Pharmaceuticals, Insys



Therapeutics, Mallinckrodt Pharmaceuticals, Allergan (f/k/a Actavis), Watson Pharmaceuticals, Amerisourcebergen Corporation, Cardinal Health, Mckesson Corporation, Omnicare Distribution Center Masters Pharmaceutical, CVS Health Corporation, Walgreens, Rite Aid Corporation, and Costco.

B. Development and Scope of Problem

Today's Opioid Crisis is a problem that has been decades in the making. As the National Institute on Drug Abuse has explained,

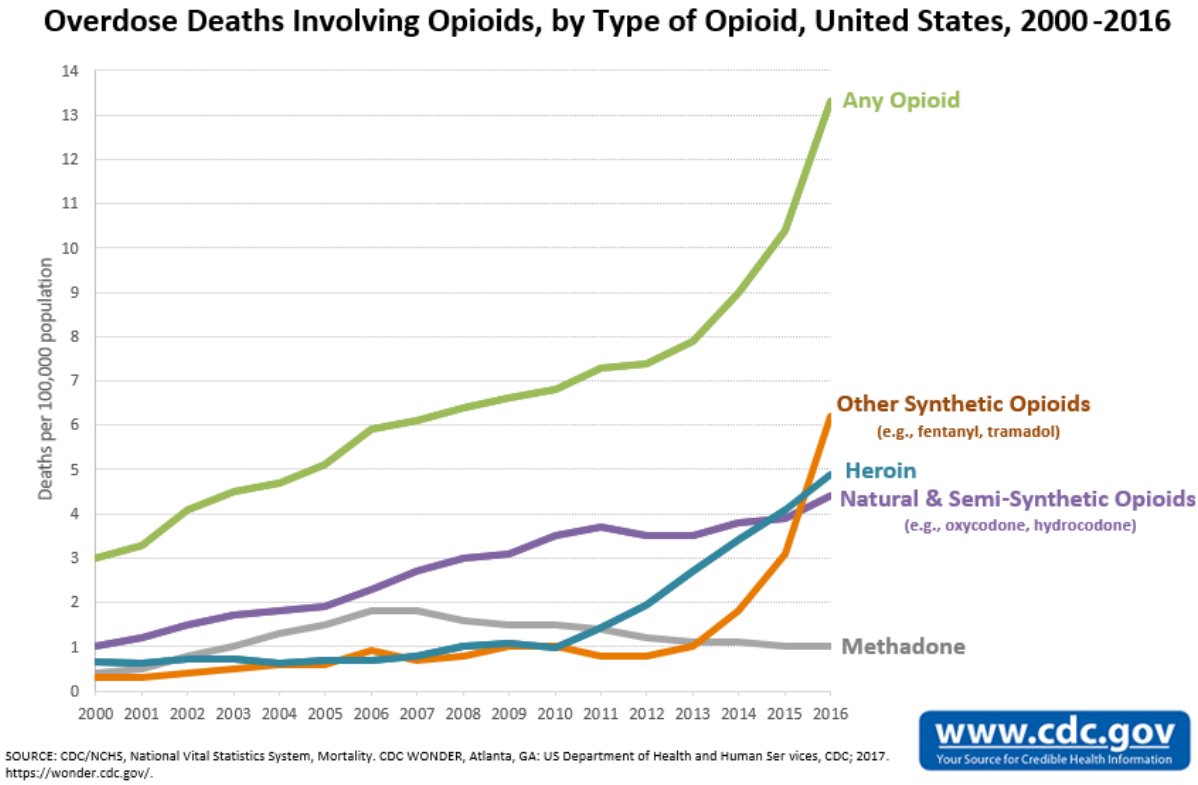
> "In the late 1990s, pharmaceutical companies reassured the medical community that patients would not become addicted to prescription opioid pain relievers, and healthcare providers began to prescribe them at greater rates. This subsequently led to widespread diversion and misuse of these medications before it became clear that these medications could indeed be highly addictive. Opioid overdose rates began to increase. In 2015, more than 33,000 Americans died as a result of an opioid overdose, including prescription opioids, heroin, and illicitly manufactured fentanyl, a powerful synthetic opioid. That same year, an estimated 2 million people in the United States suffered from substance use disorders related to prescription opioid pain relievers, and 591,000 suffered from a heroin use disorder (not mutually exclusive)."

(See National Institute on Drug Abuse, "Opioid Overdose Crisis – How did this happen?", at <https://www.drugabuse.gov/drugs-abuse/opioids/opioid-overdose-crisis>.) Recent statistics show that roughly 21 to 29 percent of patients prescribed opioids for chronic pain misuse them; between 8 and 12 percent develop an opioid use disorder; an estimated 4 to 6 percent who misuse prescription opioids transition to heroin; and about 80 percent of people who use heroin first misused prescription opioids. See National Institute on Drug Abuse, "Opioid Overdose Crisis – What do we know about the opioid crisis?", at <https://www.drugabuse.gov/drugs-abuse/opioids/opioid-overdose-crisis>.

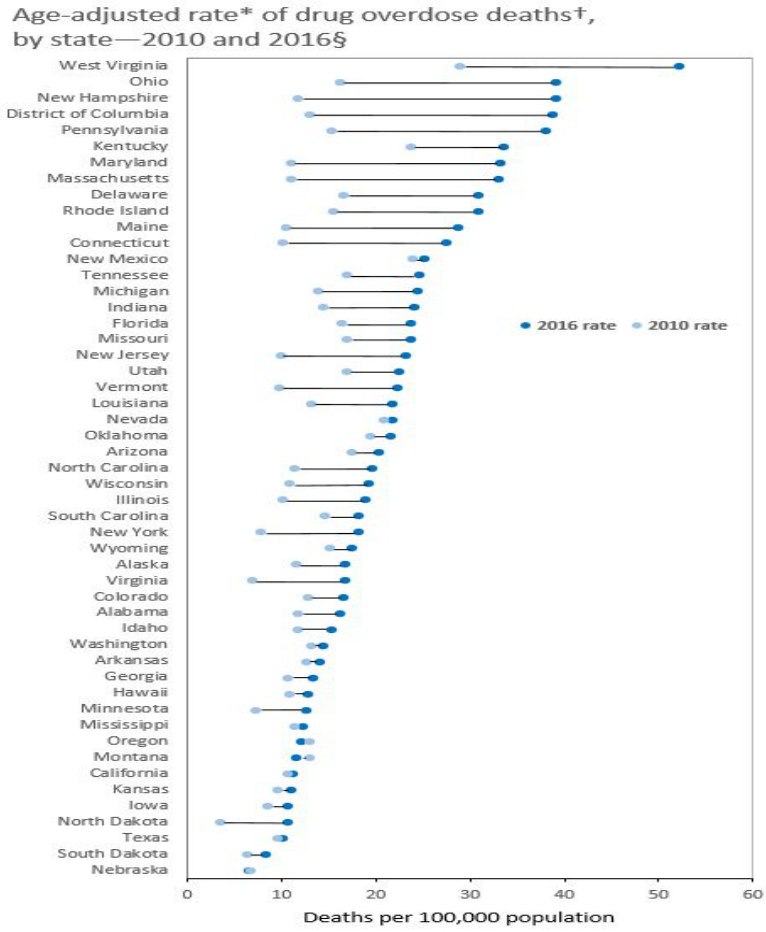
The CDC's Annual Surveillance Report of Drug-Related Risks and Outcomes indicates that between 1999 and 2016, more than 630,000 people died from a drug overdose in the United States, but that the crisis has come in waves.

> "The current epidemic of drug overdoses began in the 1990s with overdose deaths involving prescription opioids, driven by dramatic increases in prescribing of opioids for chronic pain. In 2010, rapid increases in overdose deaths involving heroin marked the second wave of opioid overdose deaths. The third wave began in 2013, when overdose deaths involving synthetic opioids, particularly those involving illicitly manufactured fentanyl, began to increase significantly. In addition to deaths, nonfatal overdoses from both prescription and illicit drugs are responsible for increasing emergency department visits and hospital admissions."

Victims of this latest wave have included people in the public eye, such as actors Heath Ledger and Philip Seymour Hoffman, musicians Prince and Tom Petty, as well as thousands of ordinary Americans.



Although the Opioid Crisis is often associated in the popular imagination with rural populations in particular regions, such as Appalachia and New England, and states such as Ohio and West Virginia, it is truly a national problem. The National Institute on Drug Abuse reports that opioid overdoses increased 30 percent from July 2016 through September 2017 in 52 areas in 45 states. Opioid overdoses increased 70 percent from July 2016 through September 2017 in the Midwest. In large cities in 16 states, Opioid overdoses increased by 54 percent. Nationwide, the incidence of drug overdose deaths continues to rise, reaching a record number of 71,568 deaths in 2017.



The costs associated with the epidemic are enormous by any standard. The cost to health insurers is estimated to be $72 billion, annually. The President's Council of Economic Advisors has calculated the cost of the crisis, in 2015 alone, to be $504,000,000. This number is comparable to the combined annual budgets of the states of California, Texas, New York and New Jersey in the same period.

C. History of Liability Claims

The first claims and suits related to opiates were brought in the early 2000s against pharmaceutical manufacturers by or on behalf of individuals who claimed to have been harmed when they become addicted. Many of these actions were commenced in State courts and were dismissed or settled.

In addition, by the mid-2000s, numerous state and federal regulators had commenced proceedings or investigations against certain manufacturers. In 2007, Purdue Frederick Company, Inc. settled criminal and civil charges against it for misbranding Oxycontin and agreed to pay a criminal fine of $635,000,000. As part of the settlement, Purdue Frederick entered into a Corporate Integrity Agreement with the Office of the Inspector General of the United States Department of Health and Human Services, 26 states and the District of Columbia that required Purdue to ensure that its marketing was fair and accurate and to monitor and report on its compliance with the Agreement.

Beginning in 2014, numerous pharmaceutical manufacturers, distributors and retailers, including pharmacies, saw themselves named as defendants in actions commenced across the United States by States, counties, cities, towns and others, relating to opioid abuse and its effects. In 2017, certain actions were transferred to the United States District Court for the Northern District of Ohio, for consolidated or consolidated pre-trial proceedings in a Multi-District Litigation ("MDL"). Others have been subsequently transferred, and today there are over 1,100 actions pending in the MDL and in other state jurisdictions. At least 41 states have sued. Additional suits are filed almost weekly. President Trump has expressed his interest in the U.S. government bringing a similar suit of its own.

The Complaints assert various causes of action against the Manufacturer Defendants, including public nuisance, negligence per se, negligence, civil conspiracy, deceptive marketing, deceptive and unfair business practices, and violation of the Racketeer Influenced and Corrupt Practices Act ("Civil RICO"). Many of the Complaints also include similar causes of action brought under State statutes. Some include causes of action designated as fraud and/or intentional misrepresentation. A small number of actions also assert claims against individual doctors accused of operating so-called "pill mills".

The states, counties and municipalities in these actions seek injunctive relief and recovery of monetary damages for economic harm incurred due to various increased costs, such as costs for:

- providing medical and additional therapeutic care and prescription drug purchases;
- other treatments for patients suffering from opioid-related addiction or disease, including overdoses and deaths;
- costs for providing treatment, counseling and rehabilitation services;
- costs for providing treatment of infants born with opioid-related medical conditions and other child welfare needs;
- costs associated with law enforcement and public safety relating to the opioid epidemic; and
- costs for the loss of tax revenue.

The plaintiffs allege many types of wrongful conduct by the defendants that resulted in the plaintiffs' damages. Typical allegations claim false and deceptive marketing of opioids by spending millions of dollars to sponsor purportedly neutral medical boards and foundations that educated doctors and set guidelines for the use of opioids in order to promote the liberal prescribing of opioids by making false and deceptive statements about the risks and benefits of opioids for treatment of chronic pain. Some complaints allege false and misleading claims, contrary to the language on their drugs' labels, regarding the risks of using their drugs that: (1) downplayed the serious risk of addiction; (2) created and promoted the concept of "pseudo addiction" when signs of actual addiction began appearing and advocated that the signs of addiction should be treated with more opioids; (3) exaggerated the effectiveness of screening tools to prevent addiction; (4) claimed that opioid dependence and withdrawal are easily managed; (5) denied the risks of higher opioid dosages; and (6) exaggerated the effectiveness of "abuse-deterrent" opioid formulations to prevent abuse and addiction. Complaints also allege that defendants falsely touted the benefits of long-term opioid use, including the ability of opioids to improve patient's function and quality of life, even though there was no scientifically reliable evidence to support the defendants' claims.

D. Current Status of Opioid Litigation

There are currently over 1100 opioid-related cases associated within the MDL styled In re National Prescription Opiate Litigation, which is assigned to United States District Judge Dan Polster of the United States District Court for the Northern District of Ohio, located in Cleveland, Ohio.

The MDL is proceeding in accordance with a Case Management Order ("CMO") issued by Judge Polster in April 2018. CMO One established a case track system, whereby cases are, or will be, assigned to tracks within which discovery and motion practice will go forward as directed by the Court. Only one track was established by the Order. Track One includes three separate cases commenced in the United States District Court for the Northern District of Ohio by The County of Summit, Ohio, The County of Cuyahoga, Ohio, and the City of Cleveland. The CMO sets for deadlines for discovery, depositions, and motions in Track One cases, and gives a tentative date for the beginning of a consolidated trial. The parties in the Track One cases will conduct written discovery and depositions pursuant to the Order. The Order also provides a briefing schedule for motions on threshold legal issues on common claims in certain cases the Court selected as representative. In their briefs, defendants seek to dismiss complaints, or selected claims. CMO One explicitly indicates that there will be coordination of the MDL with other State Court proceedings.

One key to the course of the litigation will be the use of a rich database maintained by the U.S. government that tracks sales of controlled substances (the "ARCOS database"). It is anticipated that this data will reveal whether companies neglected or ignored indications that their products were being abused.

There are at least another 200 State cases in other courts throughout the United States. These non-MDL cases are pending in state courts including those in New York, Illinois, Pennsylvania, Connecticut and others. Certain state Attorneys General have commenced actions against some or all of the same defendants. In addition to various common law claims, the actions also assert claims under states' unfair business practices and deceptive advertising statutes.

For example, in New York, twenty-three counties, the City of New York and the state's Attorney General have commenced opioid-related actions. Plaintiffs filed a Master Long Form Complaint and Jury Demand (the "Master Complaint") setting forth questions of fact and law common to all coordinated actions. The Master Complaint asserts 7 causes of action sounding in Deceptive Acts and Practices (NY GBL § 349); False Advertising (NY GBL § 350); Public Nuisance; Violation of New York Social Services Law; Fraud; Unjust Enrichment; and Negligence.

The MDL and non-MDL Opioid Litigations raise numerous legal issues, such as whether plaintiffs' claims are preempted by federal law and regulation; whether claims are barred under the learned intermediary doctrine; whether the complaints meet standards for pleading fraud; whether statutes of limitations bar claims; and whether other doctrines bar or limit recovery.

E. Limited Developments regarding insurance coverage for claims

Unsurprisingly, the claims giving rise to this opioid litigation have raised associated questions as to the defendants' insurers' obligations, as well. The limited number of decisions has addressed various issues, sometimes coming to conflicting conclusions.

- Do government claims seek damages because of bodily injury? Cincinnati Insurance Company, Plaintiff v. Richie Enterprises LLC, Defendant, 2014 WL 3513211 (W.D.

Kentucky 2014) (no); Cincinnati Ins. Co. v. H.D. Smith, L.L.C., 829 F.3d 771 (7th Cir. 2015) (yes).

- Do government claims seek damages arising from an "occurrence"? Liberty Mutual Fire Ins. Co. v. JM Smith Corporation; Smith Drug Company Inc., 602 Fed. Appx. 115 (4th Cir. 2015) (yes); The Traveler's Property Casualty Company of America et al., Plaintiffs and Respondents v. Actavis, Inc., et al., Defendants and Appellants, 16 Cal.App.5th 10226 (Cal. Ct.App. 2017) (yes).
- Do exclusions bar government claims? The Traveler's Property Casualty Company of America et al. v. Anda, Inc., et al., 658 Fed.Appx. 955 (11th Cir. 2017); The Traveler's Property Casualty Company of America et al., Plaintiffs and Respondents v. Actavis, Inc., et al., Defendants and Appellants, 16 Cal.App.5th 10226 (Cal. Ct.App. 2017) (Products exclusions).

In some cases, unanswered insurance coverage questions may be addressed using analogous decisions from prior pharmaceutical-related claims, or even other mass tort litigation, such as the epic Tobacco Litigation. Some coverage litigation regarding primary coverage for earlier phases of opioid-related litigation also exists, but it is yet to be determined whether and how such decisions may apply.

Conclusions and Remarks

The United States Opioid Crisis demands action but Opioid Litigation now pending in federal and state courts may give only some relief. Many ideas have been advanced for combatting the opioid epidemic. Some think new laws and regulations should put strict limits on the dosages of opioid prescriptions or length of time they can be used. Others suggest changing incentives and default practices in the medical establishment to curtail prescriptions in the first instance. Still others promote alternatives to pharmaceuticals for treating pain. However, none of these proposals can change the past or restore what has been lost.

Judge Polster recognized that the MDL is an imperfect approach to addressing a problem of enormous size and scope, stating:

> I've handled and managed two other MDLs, and I'm familiar with many of the others that my colleagues have handled around the country. But this is not a traditional MDL. It generally focuses on something unfortunate that's happened in the past, and figuring out how it happened, why it happened, who might be responsible, and what to do about it.
>
> What's happening in our country with the opioid crisis is present and ongoing. I did a little math. Since we're losing more than 50,000 of our citizens every year, about 150 Americans are going to die today, just today, while we're meeting.
>
> And in my humble opinion, everyone shares some of the responsibility, and no one has done enough to abate it. That includes the manufacturers, the distributors, the pharmacies, the doctors, the federal government and state government, local governments, hospitals, third-party payors, and individuals. Just about everyone we've got on both sides of the equation in this case.

> The federal court is probably the least likely branch of government to try and tackle this, but candidly, the other branches of government, federal and state, have punted. So it's here.

(Transcript of Proceedings In re National Prescription Opioid Litigation, Case No. 1:17-CV-2804, January 9, 2018.)

Americans, and the world, will watch the proceedings in Cleveland and in courts throughout the country, with great interest. However, it is unclear how resolution of the insurance claims and litigation will actually impact the continuing growth of addiction and social despair brought on by this crisis.

Thomas R. Maeglin
Abrams, Gorelick, Freidman & Jacobson, LLP
One Battery Park Plaza, 4th Floor
New York, New York 10004
(212) 422-1200
tmaeglin@agfjlaw.com

Glenn A. Jacobson
Abrams, Gorelick, Freidman
& Jacobson, LLP
One Battery Park Plaza, 4th Floor
New York, New York 10004
(212) 422-1200
gjacobson@agfjlaw.com