

Current & Developing Trends in Product Liability

Bradley C. Nahrstadt
Lipe Lyons Murphy Nahrstadt & Pontikis Ltd.
230 W. Monroe Street, Suite 2260
Chicago, Illinois 60606
(312) 448-6230
bcn@lipelyons.com

Driverless Cars

- It is projected that over the next decade, spurred by new state laws permitting the operation of autonomous vehicles and by continued investment in research and development, autonomous vehicles will become widespread.



- 9 states (CA, CO, GA, NC, NV, MI, TN, TX and FL) and the District of Columbia have passed legislation allowing for autonomous vehicles on the roadways.
- The California, Georgia, North Carolina, Tennessee and Texas statutes are silent on the issue of liability.
- The D.C., Florida, Nevada and Michigan statutes contain language protecting original manufacturers from liability for defects introduced on the aftermarket by a third party who converts a non-autonomous vehicle into an autonomous vehicle.
- The Colorado statute states that “liability for a crash involving an automated driving system driving a motor vehicle that is not under human control is determined in accordance with applicable state, federal and common law.”

- 24 other states are considering legislation that would allow autonomous vehicles on their highways.
- IL HB 2747 and SB 1432
 - Fully autonomous vehicles may operate upon the highways of the state, regardless of whether a human operator is physically present in the vehicle
 - Each FAV must bear a manufacturer's certification label indicating that at the time the vehicle was manufactured, it had been certified to be in compliance with all applicable federal motor vehicle safety standards
 - Liability for incidents involving an FAV shall be determined under existing product liability laws or common law negligence principles.

- A Senate bill, if passed, would free autonomous-car makers from some existing safety standards and pre-empt states from creating their own vehicle safety laws.
- Similar legislation has been passed in the House of Representatives.
- The Senate version has passed a committee vote but hasn't reached a full floor vote.

- May 7, 2016, the driver of a Tesla Model S was killed when a tractor-trailer turned left in front of him. The car was in autopilot mode at the time of the crash.
- March 2018, a Tesla Model X collided with a highway median in CA. The driver died in the crash. The car was in autopilot mode at the time of the crash.



© Associated Press

- On March 18, 2018 an Uber car, a Volvo XC90 sport utility vehicle outfitted with the company's sensing system, was in autonomous mode with a human safety driver behind the wheel when it struck and killed a pedestrian in Tempe, AZ.
- Uber suspended the testing of all autonomous cars in Tempe, Pittsburg, San Francisco and Toronto.

- In the “good old days”, when two cars that were being driven by individuals collided, a negligence action was typically brought against the driver who caused the accident.
- Driverless cars are going to shift the liability from a negligent driver toward manufacturers, software developers, data providers and component suppliers.

- Potential claims:

- Negligence

- Manufacturer was negligent in design and/or manufacture of the vehicle

- Strict Product Liability

- Manufacturing defect: automatic braking system contains a glitch
 - Design defect: accident occurs because driver does not take over control quickly enough; Π argues design defect because the vehicle should have been designed to provide the driver with more advanced notice
 - Failure to warn: software upgrades
 - If malfunction in the software caused the crash, can the plaintiff bring a strict products liability suit since software may not be a product?

– Misrepresentation

- Manufacturer advertises that a human driver will “very rarely” need to take over control of the vehicle
- If the driver has to take over every 3 to 4 minutes, he or she could bring a claim for misrepresentation

– Breach of Warranty

- Manufacturer advertises that its autonomous vehicle parallel parks itself just as well at night as during the day
- If that turns out to be untrue the owner could bring a breach of express warranty claim

Three-D Printers

- In 2017, the 3D printing market in the U.S. was \$8.8 billion.
- By 2021 that market is projected to increase to \$26.5 billion.
- Each year, 50,000 people worldwide benefit from customized surgical equipment made from 3D printing.



- The parties involved in the 3D printing supply chain—any of whom may be implicated in the event of a potential product liability issue, include:
 - The manufacturer or supplier of the 3D printer
 - The manufacturer or supplier of the 3D printing material
 - The printer owner
 - The person who designed or sold the original object upon which the 3D printing design is based
 - The person who created or shared the CAD blueprint of the object
 - The person who printed the object
 - The person who sold the printed object

- Interesting product issues in 3D printing cases:



- Was there a design defect in the original object or a design defect in the CAD blueprint?
- Did the 3D printer fail to properly implement the design in creating the object?
- Was the material used to print the object defective?

- Is the person who supplied the product a “seller”?
 - Layperson or recreational 3D printing enthusiast is not likely going to be considered a seller, although a routine vendor of 3D printed goods likely would be.
- Federal pre-emption
 - The FDA has regulatory authority over 3D printed medical devices.
 - The FDA is beginning to issue technical considerations and guidance for 3D printing.

Medical Device Cybersecurity



- January 9, 2016, the FDA issued a Safety Communication setting out the potential risks that could be caused by vulnerabilities in certain St. Jude Medical cardiac devices.
- The devices transmit data directly to physicians to allow direct patient and device monitoring.

- FDA warned that vulnerabilities in the devices could allow unauthorized users to remotely access the device and alter the devices' programming.
- In December of 2017, the FDA published guidance addressing cybersecurity for medical devices already on the market.
- Calls for manufacturers to monitor devices on the market, assess how vulnerabilities could affect patients, use software patches to mitigate risk and work with researches to understand potential cyber threats.

- Manufacturers that do not address cybersecurity issues may face claims for:

- Negligence
- Breach of warranty
- Strict product liability
 - Defective design
 - Failure to warn



Innovator-Liability Theory

- “Innovator liability” is a theory pursued by plaintiffs who contend that a brand-name drug manufacturer owes a duty to warn plaintiffs—or their physicians—of supposed dangers shared in common with a generic formulation of the innovator’s branded drug.



- Until recently, many in the legal community had taken for granted that innovator liability was a dead theory.
- Approximately 100 decisions, applying the law of approximately 28 states, had rejected it.
- The problem: most of the courts that rejected the theory were federal courts, predicting state law on the issue, or state courts at an intermediate level.

- In April of 2017, a jury in a federal court in Illinois returned a \$3 million verdict in favor of the widow of an attorney who committed suicide days after taking a generic formulation of GlaxoSmithKline's drug Paxil. *Dolin v. Smith-kline Beecham Corp.*, Case No. 12-CV-6403 (N.D. Ill. 2017).
- In late 2017, the California Supreme Court endorsed innovator liability in the case of *T.H. v. Novartis Pharmaceuticals Corp.*, 4 Cal. 5th 145, 407 P.3d 18, 226 Cal. Rptr. 3d 336 (Cal. 2017).

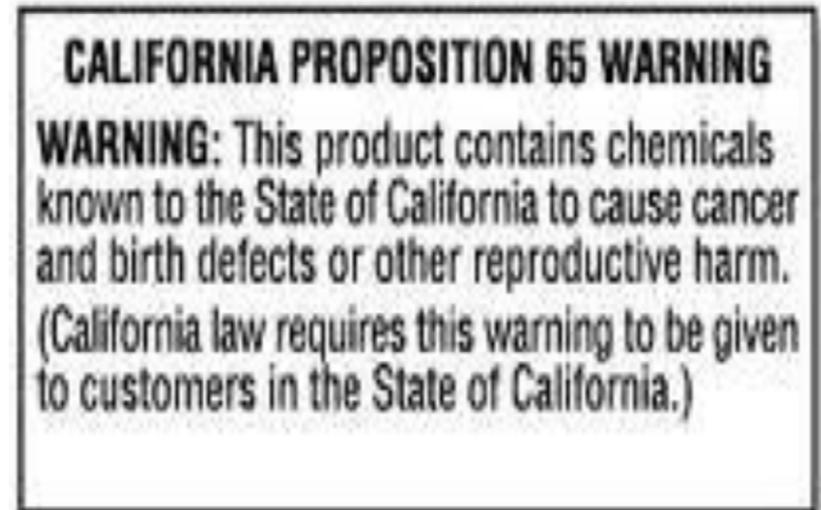
- On March 16, 2018, the Massachusetts Supreme Judicial Court gave its blessing to innovator liability in the case of *Rafferty v. Merck & Co.*, 2018 Mass. LEXIS 161 (March 16, 2018).
- The sharks are undoubtedly beginning to circle!



- Strategies to resist innovator liability:
 - Remove the case to federal court.
 - In states with statutory product liability acts, counsel should be prepared to argue that the legislature, not the courts, should be the source of new theories of product liability.
 - Develop facts showing that the plaintiff's injury was not caused by a failure to warn but rather a defect in the generic condition.

Proposition 65

- **Originated as an initiative approved by the people of California in 1986 to require businesses to provide clear and reasonable warning before exposing people to certain chemicals that exceed certain thresholds.**



- Section 25249.6 California Health and Safety:

No person in the course of doing business shall knowingly and intentionally expose any individual to a chemical known to the state to cause cancer or reproductive toxicity without first giving clear and reasonable warning to such individual.

- Broad range of chemicals on the Prop 65 list (approximately 940 as of 12/31/17).
- 25102(i) “Exposure” means to cause to ingest, inhale, contact via body surfaces or otherwise come into contact with a listed chemical.
- 25102(n) “Knowingly” refers only to knowledge of the fact that a discharge of, release of, or exposure to a chemical listed pursuant to Section 25249.8(a) of the Act is occurring. No knowledge that the discharge, release or exposure is unlawful is required.

- If there is a chemical in your product that exceeds the No Significant Risk Level (NSRL) or the No Observable Effect Level (NOEL), or in the case of reproductive effects, the Maximum Allowable Dose Level (MADL), then you must warn of the danger.



- In order to avoid confusion the Office of Environmental Health Hazard Assessment (OEHHA) issued regulations that include so-called “safe harbor” warnings that if used are presumptively sufficient.
- Not required to use the safe harbor warnings, but doing so signifies presumptive compliance with the law.

- Prop 65 was amended in August of 2016.
- New provisions take effect on August 30, 2018.
- Significantly change the content of safe harbor warning label and warnings that must be given for Internet and catalog purchases.
- Added “tailored” warnings for specific kinds of exposure: dental care, furniture, diesel engines, automobiles, recreational vessels, amusement parks, etc.

- A symbol consisting of a black exclamation point in a yellow equilateral triangle with a bold black outline. Where the sign, label or shelf tag for the product is not printed using the color yellow, the symbol may be printed in black and white. The symbol shall be placed to the left of the text of the warning, in a size no smaller than the height of the word “WARNING.”



- If the warning is NOT provided on the product itself, it must name at least one chemical for which the warning is being provided and specify whether that chemical is known to cause cancer, birth defects or reproductive harm or both.

 **WARNING**

This product can expose you to chemicals, including [name of one or more chemicals] which is [are] known to the State of California to cause cancer or birth defects or other reproductive harm. For more information, go to www.p65Warnings.ca.gov/furniture.

- Warning must be in a type size no smaller than the largest type size used for other consumer information on the product with a minimize 6-point type.
- Warnings must include a link to the appropriate Prop 65 website.
- Warning must be given in English; BUT, if a product sign, label or shelf tag used to provide a warning also contains consumer information in a language other than English, the warning must also be provided in that language.

- Can avoid specifying a chemical only if the warning is provided ON THE PRODUCT, it contains the pictogram, it identifies the potential risk (cancer or reproductive harm) and it lists the Prop 65 website:



WARNING: Cancer - www.P65Warnings.ca.gov



WARNING: Reproductive Harm - www.P65Warnings.ca.gov

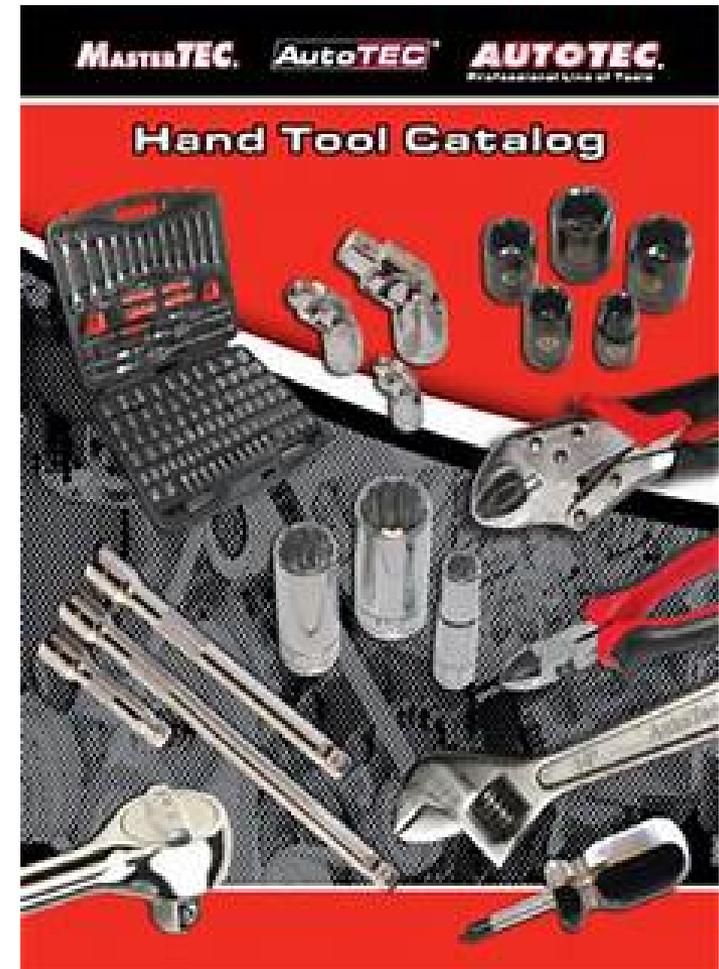
- Warnings must be provided to the consumer prior to or at the time of purchase.
- Can provide a product-specific warning, on a posted sign, shelf tag or shelf sign, at each point of display.
- Can provide a product-specific warning via any electronic device or process which automatically provides the warning to the purchaser prior to or during the purchase of the product.

- Internet Purchases.
- Warnings must be provided prior to completing a purchase:
 - Product display page
 - Give via a hyperlink using the word warning
 - Appear on the last page before the consumer pays



- This is in addition to the requirement that the warning be provided on or with the product through one of the four methods described in § 25602(a):
 - Point of display warnings
 - Warnings provided in store through scanner or bar code reader
 - Warnings on labels
 - On product warnings

- Catalog purchases:
 - To meet the safe harbor requirements, any business that sells products in a catalog must provide a clear and reasonable warning in the catalog in a manner that clearly associates the warning with the item(s) being purchased.
 - Warning symbol alone is NOT sufficient; cannot require the consumer to seek out the warning on a different page of the catalog



GDPR



- European Union's General Data Protection Regulation (GDPR)
- Takes effect on May 25, 2018.
- Penalties for non-compliance can be as high as 20 million Euros or 4 percent of annual worldwide turnover.

- Not limited to organizations located in the European Union.
- Applies to EU personal data processing activities of entities that are not established in the EU if such processing activities are related to (1) *the offering of goods or services to data subjects in the EU, regardless of whether a payment from a data subject is required*; or (2) the monitoring of data subjects' behavior within the European Union.

- The GDPR contains provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.
- The GDPR also regulates the exportation of personal data outside the EU.
- Personal data must be processed in a manner that is lawful, fair and transparent.
- Organizations are required to provide extensive information to data subjects in relation to the processing of their personal data.

- What types of privacy data does the GDPR protect?
 - Basic identity information such as name, address and ID numbers
 - Web data such as location, IP address, cookie data and RFID tags
 - Health and genetic data
 - Biometric data
 - Racial or ethnic data
 - Political opinions
 - Sexual orientation

- Under the GDPR:
 - Personal data must be collected for specified, explicit and legitimate purposes;
 - Personal data gathered must be adequate, relevant and limited to what is necessary;
 - Personal data must be accurate and kept up to date (reasonable steps must be taken to ensure that inaccurate data is erased or corrected);
 - Personal data must be kept in a form that permits identification for no longer than is necessary for the purposes for which the data is processed;
 - Personal data must be processed in a manner that ensures appropriate security of the data.

- Under the GDPR individuals have the right to:
 - Access their data;
 - Have their data erased (Right to be Forgotten)
 - Have their data corrected



- Companies must be able to demonstrate compliance with the GDPR's data protection principles.
- Companies must conduct mandatory data protection impact assessments.
- Companies must maintain records of their data processing activities.

- What do companies have to do to comply?
 - Appoint data protection officer(s)
 - Review and update privacy notices and terms and conditions
 - Need to set out the purposes and lawful bases for all processing activities, the data retention period, information concerning data subject rights and the right to complain to a data protection authority.

- Update Data Protection Compliance Program
- Implement or update procedures to ensure compliance with individual rights under the GDPR
- Implement standard operating procedures for GDPR obligations
- Update data breach notification protocol (under the GDPR, a company has to notify customers of a data breach within 72 hours of the breach)

- Document the company's compliance with GDPR
 - Records of processing activities;
 - Data protection by design and default;
 - Lawful bases for processing
 - Data protection impact assessments;
 - Data breach response processes.

Current & Developing Trends in Product Liability

Bradley C. Nahrstadt
Lipe Lyons Murphy Nahrstadt & Pontikis Ltd.
230 W. Monroe Street, Suite 2260
Chicago, Illinois 60606
(312) 448-6230
bcn@lipelyons.com