8: EVALUATING TORT LAW, PART 2

- data & cybersecurity laws
  - US govt has implemented data laws slowly, first applying them to most relevant sectors only
  - many states have enacted laws to cover gaps not addressed at federal level
  - notable fed laws
    - Federal Trade Commission Act (FTCA) of 1914
      - prohibits unfair or deceptive practices
      - has been applied to prohibit use of illegally obtained consumer data
    - Family Educational Rights & Privacy Act (FERPA) of 1974
      - restricts when students' educational records can be accessed
    - Computer Fraud and Abuse Act (1986)
      - prohibits accessing a computer w/o authorization
      - one of first regulations to address hacking
    - Health Insurance Portability and Accountability Act (HIPAA) of 1996
      - regulates how medical info can be stored/shared & what must be done if breach occurs
      - applies to healthcare providers, insurers, cos that process people's medical info
    - Children's Online Protection Act of 1998
      - imposes data collection & privacy requirements on websites aimed at kids under 13
    - Gramm-Leach-Bliley Act/Financial Modernization Act of 1999
      - governs collection, use, and disclosure of financial data
      - applies to financial institutions, such as banks and ins cos
    - Homeland Security Act of 2002
      - produced the Dept of Homeland Security (DHS)
      - DHS Privacy Office:
        - addresses privacy issues related to homeland security
        - responds to complaints of privacy violations
    - Federal Information Security Management Act (FISMA) of 2002
      - provides mandatory framework for federal agencies to use to develop/implement information security programs
    - Cybersecurity Information Sharing Act of 2015
      - authorizes cos to monitor and defend their information systems
      - protects cos that voluntarily share information regarding cyber threats w/ govt authorities (as long as certain guidelines are followed)
  - other key efforts:
    - implementing Payment Card Industry Data Security Standard (PCI DSS)
      - set of information policies/procedures adopted by major credit card cos
      - is **not** a law
      - is required to be adopted by bizs that process a large volume of credit card transactions
    - Executive Order 13636 - Improving Critical Infrastructure Cybersecurity
      - directs US govt to promote & incentivize the adoption of cybersecurity practices & cyberthreat information sharing
  - bizs need to be aware of laws to ensure compliance and keep customers' trust

- 3 areas of data protection law
  - data privacy
    - involves the appropriate use or access of data
    - can cover:
      - what info can be collected
      - how & whom it can be shared
      - how it must be disposed of
    - ex: California Consumer Privacy Act (CCPA)
      - one of strictest data privacy laws in US
      - provides consumers w/ several rights:
        - ability to find out what info has been or is being collected & how
        - right to know if info is sold or disclosed & to whom
        - option to opt out of biz being able to sell their info
        - option to have their info deleted (w/ some exceptions)
        - right to not be discriminated against for exercising these rights
      - viewed by most companies as the de facto (default) standard
      - model for other states' privacy laws
  - breach notification
    - all states require cos to notify people of security breaches if their personally identifiable info (PII) might have been exposed
    - PII includes any unique info (ex: name, address, social security #, etc.) that requires safekeeping & confidentiality
    - *security breach* includes any unauthorized access of computerized personal info
    - safe harbor:
      - easing or eliminating penalties or compliance requirements if good-faith effort is made to provide intended protection of the law
      - many states waive notification requirements for **encrypted** data
  - data security
    - involves the protection of data from unauthorized access
    - laws vary widely from state to state
    - examples of what laws might require a co to have:
      - written information-security procedures
      - encryption of personal info records communicated over wireless networks or stored on personal devices
      - annual review of security measures
      - compliance w/ PCI DSS standards
      - written cybersecurity procedures
      - chief information security officer (responsible for protecting data & info systems)
    - *cybersecurity*: involves the protection of data from unauthorized access **through the internet**
- General Data Protection Regulation (GDPR)
  - comprehensive set of formal data protection rules established under the European Union (EU)
  - viewed as the global model of standard for pers data regulation
    - applies to cos operating **in** EU or that process data from EU residents
  - based on fundamental premise that individuals own their own pers data

        - requirements:
            - collect only the min amt of data needed to perform a task
            - collect & store data only if person gives consent
            - keep data only as long as necessary to perform a task
            - erase data upon that person's request
            - breaches must be reported to authorities & individuals w/i 72 hrs
            - allow people to opt out of having a machine make decisions about them
            - document what you are doing to comply w/ GDPR
            - data must be tracked as it moves through an organization
            - perform assessments to ID security vulnerabilities
    - best practices
        - establish a culture of strict security
        - appoint someone to be in charge of data security (such as chief info security officer)
        - collect & store only minimum data needed to complete a task
        - limit # of employees who can access pers data
        - install security features on personal devices
        - enforce security pol regarding any devices left unattended or unlocked
        - train employees on:
            - precautions to take before connecting to public networks
            - when it is ok to plug external devices into work computers
            - phishing or malicious emails
            - how to properly destroy pers data records that aren't needed anymore
            - reporting suspicious emails or customers
        - establish online privacy pol that explains how pers info will be used and controlled by co
        - if data is exposed, use it as a teachable moment w/o calling out who was at fault
- strict liab/absolute liab:
    - being held liab even if you acted reasonably & had no fault
    - usually applies to situations considered extremely dangerous or abnormal
    - may extend to things artificially brought onto land
    - liab can extend to non-users (bystanders who weren't the ones using the product or object)
    - ultrahazardous activity:
        - abnormally dangerous activity that can't be performed safely even w/ reasonable care
        - plaintiff must prove 3 circumstances:
            - high degree of risk of serious harm
            - activity can't be performed w/o high degree of risk
            - activity doesn't normally occur in area where it is conducted
        - performer is liab if any harm results
        - includes liab for dangerous substances brought onto real prop that escapes & causes dmg
    - pets
        - may apply if owner knew of animal's propensity to harm/attack
        - law applies differently to domestic vs. wild animals
            - law differentiates btwn both based on **local customs**
            - owner of **wild** animal is strictly liab for any acts/dmgs caused by it
    - toxic torts
        - liab based on exposing others to a toxic substance
        - generally established by statute rather than common law

- product liability
  - ways you can be liab w/ respect to your products
    - misrepresentation
    - breach of warranty
    - strict liab & neg
      - plaintiff must prove product was cause of their dmgs
      - types of product defects
        - defect in manufacture or assembly
          - product doesn't correspond to orig design/specifications
          - includes use of poor-quality materials or shoddy assembly work
        - defect in design (design itself is faulty)
        - failure to warn users
          - 3 factors
            - degree of danger
            - knowledge of danger
            - foreseeability of dangerous use
          - ex: if person knew faulty switch could cause burns to user w/ wet hands, **not** be liab under common law but **is** liab under today's law
      - manufacturers **not** liab for defect occurring after product left manufacturer's possession
  - defenses
    - state of art
      - product was safe according to existing science & knowledge at time product was made
      - if there was no indication of danger or no technique to obtain knowledge of danger, manufacturer has no reason to prevent production or use
      - **not a complete defense**
      - ex: former use of asbestos in construction, which is now known to be danger to health
    - you complied w/ statutes/regulations
    - you complied w/ product specs
      - manufacturer generally **not** liab for products built to someone else's specs
    - open & obvious danger (user should have known of danger)
    - plaintiff's knowledge (plaintiff has equal knowledge of risks as manufacturer)
    - comparative neg
      - <u>active neg/assumption of risk</u>: voluntary use of product w/ knowledge of existing defect
      - <u>passive neg</u>:
        - plaintiff's failure to discover a product's defect or to guard against poss defect
        - ex: wire was clearly frayed but plaintiff didn't notice
    - misuse of product
    - alteration of product
- types of dmgs that can be awarded
  - compensatory dmgs
    - <u>special dmgs</u>: actual costs of dmgs incurred, out of pocket expenses & loss of wages/earnings
    - <u>general dmgs</u>: value of pain, suffering, distress
    - *emotional distress dmg* includes recurring nightmares & phantom pains
  - <u>punitive dmgs</u>
    - awarded to punish defendant if either:
      - defendant actually intended to cause harm
      - defendant acted maliciously, fraudulently, or outrageously

- wrongful death action
  - filed by survivors of a deceased party
  - survival statutes: gives a deceased person's estate the right to file for dmgs that the person incurred btwn date of inj and death

- other tort concepts
  - joint tortfeasors (joint & several)
    - an innocent party can collect 100% of damages from any negligent party
    - negligent party who paid 100% then pursues other negligent parties for appropriate portion
      - contribution: right of tortfeasor who has paid more than his share of dmgs to collect from other tortfeasors
    - prevents innocent party from being delayed if negligent parties dispute how to split liab
    - Uniform Contribution Among Joint Tortfeasors Act (UCAJTFA)
  - expanded liab concepts (when multiple companies can be liab)
    - enterprise liab (industry-wide liab):
      - each member of an industry can liab for manufacturing harmful/defective product if specific manufacturer at fault can't be ID'd
      - works like joint & several liability, so plaintiff could win 100% from single defendant
    - alternative liab:
      - applies when there are several defendants but unk which one is at fault
      - shifts burden of proof to defendants, who must prove they didn't cause harm or that another defendant did
    - mkt share liab:
      - defendants liab for pro rata mkt share unless they prove they couldn't have made product involved
      - similar to enterprise liab, but defendant max exposure is mkt share % rather than 100%
    - concert of action: applies when multiple defendants had to have act together or cooperatively to create the dangerous product/event (ex: racing)
    - conspiracy: when 2+ parties work together to purposely commit unlawful act
    - *joint venture*:
      - biz association formed by two or more parties to accomplish a project
      - to sue all parties to the joint venture, plaintiff must prove 4 elements:
        - agreement by parties to associate for biz activity
        - profits/losses shared by all parties
        - joint control of venture by all parties
        - contribution to the venture's assets by all party
  - vicarious liab (when one party is liab for another's actions)
    - principal & agent (when one party was authorized to act on another's behalf)
    - employer & employee
    - parent & child
      - parent **generally not** liab for minor child's torts
      - exceptions:
        - child acted as parent's agent/employee
        - negligent entrustment: involves dangerous instrument (ex: gun/car) that parent gave to child when parent should've expected child can cause harm
        - negligent supervision: failure to reasonably keep child from causing harm
        - (some jurisdictions) family purpose doctrine: owner of car is liab for dmgs caused by any family member driving that car

- good Samaritan law: protects those giving emergency assistance from ordinary neg, but **not gross neg**
- class actions & mass tort litigation
  - class action: when 1 or a few parties represent interest of an entire class of people in litigation
  - 4 considerations
    - numerosity (too many plaintiffs to practically hear each case separately)
    - commonality (well-defined common legal elements)
    - typicality
      - claims, defenses, dmgs sought must be basically the same for all members
      - ex: if most members in asbestos class action suit suffered moderate respiratory problems but one person suffered stage 4 cancer, he would not fit this trait
    - adequacy of representation (named parties must fairly & adequately protect interests of non-named members)

- US laws that affect int'l biz
  - Internal Revenue Code (tax code)
    - foreign tax credits
    - *repatriation of earnings*: process by which US parent co moves earnings from foreign affiliates back to US parent co or stockholders
    - corp tax brackets
  - Foreign Corrupt Practices Act
    - prohibits payments/bribes to foreign officials to obtain or keep biz
    - requires cos that list their securities (stocks) in the US to meet certain acct provisions
    - puts US cos at disadvantage
  - Patriot Act
    - to deter & punish terrorist acts in US
    - increases surveillance & investigative powers of US law enforcement agencies
    - Section 215: broadens FBI's ability to obtain biz records pursuant to court order
    - Sections 351-366: permits govt access to info from banks that might relate to terrorism
    - Section 351: allows Sec of Treas to impose sanctions, including cutting off all dealings w/ US financial institutions/banks in foreign nations whose bank secrecy laws deny info to US agencies
    - Section 352:
      - prohibits financial institutions from knowingly becoming involved in unlawful transactions w/ suspected terrorists
      - requires cos to:
        - incorporate internal policies/procedures/controls based on money-laundering risks
        - designate compliance officer
        - establish ongoing training programs & audit functions to test programs