Dittman v. UPMC

A Discussion of the Economic Loss Doctrine and Legal Duty to Protect Personal Information

"Defending the Corporate House"
Central PA Association of Corporate Counsel
April 25, 2019

Carol Steinour Young
Devin Chwastyk

Pennsylvania: Evolution of the Economic Loss Doctrine

- **1927 – Roots of economic loss doctrine first recognized in *Robins Dry Dock and Repair Company v. Flint*, 275 U.S. 303**

- **1985 - PA Superior Court cites doctrine in *Aikens v. Baltimore & O.R. Co.***

Pennsylvania: Evolution of the Economic Loss Doctrine

- **2005 – PA Supreme Court (Bilt-Rite) case determined where it is foreseeable that a third person will rely upon information provided by the engineer in his employment or contractual engagement by an owner, that third person is entitled to sue the design professional for economic losses under a theory of negligent misrepresentation.**

- **Note – the plaintiff did not file a claim for negligence**

Pennsylvania: Evolution of the Economic Loss Doctrine

- **2006 – PA Superior Court applies Bilt-Rite principles to Excavation Technologies case – it is later appealed to Supreme Court.**
- **2009 – PA Supreme Court in *Excavation Technologies, Inc. v. Columbia Gas Company of Pennsylvania*, 2009 W.L. 5103605 (Pa. 2009), declined to expand the exception to the economic loss doctrine which it had created in the seminal case of Bilt-Rite Contractors. In the court's Opinion, the Judges noted it should be the duty of the Legislature to impose liability.**

Pennsylvania: *Dittman vs. UPMC*

- *Dittman vs. UPMC*: class action litigation by employees arising from 2014 criminal hack of the University of Pittsburgh Medical Center's computer systems
- Hackers accessed personal and financial data stored by UPMC on the hospital's HR systems
- Exposure of **Social Security numbers, birthdates, confidential tax information, addresses, salaries, and bank account information**
- Employees alleged that this information was used to file fraudulent tax returns

Pennsylvania: *Dittman vs. UPMC*

- **Plaintiffs brought claims in PA state court for negligence and breach of an implied contract**
  - Employees alleged UPMC breached its duty to use reasonable care "by failing to adopt, implement, and maintain adequate security measures, failing to adequately monitor the security of its network, allowing unauthorized access to Employees' information, and failing to recognize in a timely manner that Employees' information had been compromised."

Pennsylvania: *Dittman vs. UPMC*

- 2015: Court of Common Pleas of Allegheny County:
  - Judge Wettick applies economic loss doctrine – “only losses sustained are economic losses”
  - Pennsylvania law did not recognize a duty to secure employee data
  - Pennsylvania courts should not create "a new affirmative duty of care that would allow data breach actions to recover damages recognized in common law negligence actions."
  - Doing so would open the floodgates to "hundreds of thousands of lawsuits by persons whose confidential information may be in the hands of third persons.“

Pennsylvania: *Dittman vs. UPMC*

- 2015: Court of Common Pleas of Allegheny County:
  - "Clearly, the judicial system is not equipped to handle this increased case load of negligence actions. Courts will not adopt a proposed solution that will overwhelm Pennsylvania's judicial system."
  - For-profit and nonprofit entities "would be required to expend substantial resources responding to the resulting lawsuits. These entities are victims of the same criminal activity as the plaintiffs. The courts should not, without guidance from the Legislature, create a body of law that does not allow entities that are victims of criminal activity to get on with their businesses."

Pennsylvania: *Dittman vs. UPMC*

- 2017: Pennsylvania Superior Court affirms the trial court ruling

- November 2018: Pennsylvania Supreme Court reverses
  - Court is persuaded by Plaintiffs' allegations that—as a condition of employment at UPMC—they were required to provide certain financial and personal information. They further alleged that UPMC collected and stored that information on its internet-accessible computer system without the use of adequate security measures, including proper encryption, adequate firewalls, or adequate authentication protocols.

Pennsylvania: *Dittman vs. UPMC*

- Legal implications of the Supreme Court's ruling
  - Duty to protect PII: The court held that where an employer's affirmatively undertakes a collection of employees' personal information, the employer has a duty of reasonable care to secure its employees' personal information "against an unreasonable risk of harm arising out of the employer's data collection practices."

Pennsylvania: *Dittman vs. UPMC*

- Legal implications of the Supreme Court's ruling
  - Departure from economic loss doctrine: Old formulation of the economic loss doctrine focused on type of damages but on the nature of the duty
    - **Trial court: "no cause of action exists for negligence that results solely in economic losses unaccompanied by physical injury or property damage."**
    - **Supreme Court: "The question of whether the plaintiff may maintain an action in tort for purely economic loss turns on the determination of the source of the duty."**

Pennsylvania: *Dittman vs. UPMC*

- Legal implications of the Supreme Court's ruling
  - Departure from economic loss doctrine:
    - **"A breach of a duty which arises under the provisions of a contract between the parties must be redressed under contract, and a tort action will not lie."**
    - **"A breach of duty arising independently of any contract duties between the parties, however, may support a tort action."**
  - Merger of the economic loss doctrine with the gist of the action doctrine?
    - **Or, demise of both doctrines?**

Pennsylvania: *Dittman vs. UPMC*

- Legal implications of the Supreme Court's ruling
  - Judicially-created data protection obligation to act with reasonable care in collecting and storing personal and financial information
    - **Departure from statutory/regulatory approach and reactive obligations on businesses**
      - Proactive: Legislative data security standards (CA, MA, Ohio Safe Harbor Law, NY Department of Financial Services)
      - Reactive: 50 state breach notification laws
  - "Personal and financial information" not defined, but broader than the PA Breach Notification Act
    - **Names, birth dates, Social Security numbers, addresses, tax forms, and bank account information**

Pennsylvania: *Dittman vs. UPMC*

- **Post-*Dittman* Developments**
  - Subsequent cases:
    - ***Spade v. U.S.*** **(3rd Cir.): vacating dismissal of negligent disclosure of PII claim**
    - ***Pflendler v. PNC Bank*** **(3rd Cir.): *Dittman* "clarify[ied] that the applicability of the economic-loss doctrine depends on whether the duty at issue "arises independently of any contractual duties between the parties."**
    - ***Hanreck v. Winnebago Indus.*** **(M.D.Pa.): UTPCPL claims not barred by economic loss doctrine**
    - ***Gernhart v. Specialized Loan Servicing LLC*** **(E.D.Pa.): "The economic loss doctrine does not preclude all negligence claims seeking solely economic damages, but continues to preclude actions where the duty arises under a contract between the parties. Only where the duty arises independently of any contractual duties may a breach of that duty support a tort action."**
    - ***Southern Indep. Bank v. Fred's, Inc.*** **(M.D.Al.): "The state of Pennsylvania's economic loss rule is in doubt …"**

Pennsylvania: *Dittman vs. UPMC*

- **Practical implications of the Supreme Court's ruling:**
  - Any entity that collects and stores the sensitive information of any person likely will be subject to a duty to exercise reasonable care to safeguard it against the foreseeable risk of a data breach—even one committed by hackers.
    - **Reasonableness standard means subsequent lawsuits will not be easily dismissed by trial courts**
    - **Reasonable safeguards not defined**
  - Not limited to the employment context (clients, customers, students, patients, etc.)
  - No carve-out for small businesses – extends to all employers
  - Are we headed toward strict liability for data breaches?

Pennsylvania: *Dittman vs. UPMC*

- How can businesses avoid liability under *Dittman*?
  - Look to legislative and industry standards and best practices
    - **NYFDS, MA WISP, Ohio Safe Harbor Law**
    - **Laws require that businesses create and maintain a cybersecurity program (including written policies approved by BOD or senior management, controls, and practices) that reasonably conforms to industry-recognized cybersecurity frameworks or applicable laws and/or reasonably protects against unauthorized access/acquisition of information likely to result in a material risk of identity theft**
      - Frameworks: NIST, ISO 27000-series, CIS, PCI-DSS
      - Applicable laws (for regulated entities): HIPAA, GLBA, FISMA, HI-TECH
  - Separate IT governance and IT security functions
    - **Leadership: CISO and/or board-level responsibility**
  - Technical solutions: access controls/least privilege; encryption; MFA

Pennsylvania: *Dittman vs. UPMC*

- Legal process to avoid liability under *Dittman*
  1. **Assessment**: determine how much and what categories of PII are being collected, how, and why. Is this collection necessary and can any of it be purged?
  2. **Adoption**: written information security program, including:
     1. **Appropriate policies, such as: (a) data security policy; (b) privacy notices; (c) acceptable use policy; (d) document retention policy; (e) retention and destruction schedules; (f) vendor access and assessment policy; (i) remote access policy; (ii) BYOD policy …**
     2. **And practices: (i) disaster recovery; (ii) external media; (iii) encryption; (iv) least access controls; (v) monitoring of resources; (vi) patches and updates; (vii) passwords; (vii) change management**
  3. **Breach Response Plan**: adoption and routine testing/war-gaming
  4. **Training**: of employees upon hiring and annually thereafter
  5. **Audit**: routine audits and revisions of policies, and audits of employee compliance
  6. **Insurance**: consider scope and amount of cyber-liability coverage