New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 261—NO. 45
FRIDAY, MARCH 8, 2019

Outside Counsel

Expert Analysis

Is 'Dittman' Creating a New Common Law Privacy Obligation on Employers?

BY FREDERICK D. BRAID, LOREN L. FORREST JR., MARK S. MELODIA AND NIPUN J. PATEL

The law has spent centuries chasing technological changes. Legal rules tend to evolve from the slow accumulation of precedent or from the difficult-to-find common ground of legislative consensus. And yet, the opportunities and risks created by society's technological hares race ahead without heed to the pace of the legal tortoises. Cybersecurity vulnerabilities at U.S. companies, and the resulting problems maintaining the privacy of personal information of employees, present the latest iteration of this age-old dilemma. Courts, legislatures and regulators have attempted to define the duties of employers concerning security and privacy, and this article explores the pros and cons of each approach. In the end, without regard to who is making the legal rules, the change is upon us and certain practical steps will best serve the interests of both employers and employees in this digital era.

The Common Law Approach

The recent Pennsylvania Supreme Court landmark decision in *Dittman v. UPMC*, established a common law duty on the part of Pennsylvania employers "to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an Internet-accessible computer system." 196 A.3d 1036, 1038 (Pa. 2018). The decision saved from dismissal a putative class action premised on claims of negligence and breach of implied contract. The employees claimed that their sensitive personal identifying information (PII) was stolen from UPMC following a criminal hack. Id. at 1038-39. The *Dittman* court held that Pennsylvania common law required employers who affirmatively undertake the collection and storage of their employees' sensitive PII to implement "reasonable care" and "adequate" security measures. Id. at 1048. The opinion suggests that the duty of reasonable care includes: encrypting, establishing "adequate" firewalls, and implementing "adequate authentication protocol[s]." Id.

The *Dittman* court expressly disavowed any intention to create new affirmative duties under the law; rather, it emphasized that the holding was applying the Restatement (Second) of

FREDERICK D. BRAID *is a partner at Holland & Knight, where he heads the labor, employment and benefits group.* LOREN L. FORREST JR. *is a partner in the group.* MARK S. MELODIA *is a privacy, data security and consumer class action defense partner, and* NIPUN J. PATEL *is a partner and trial lawyer at the firm.*

Torts §302 requiring protection and reasonable care where an actor engages in affirmative conduct. Id. However, as the *Dittman* court correctly observed in reviewing UPMC's arguments, the Pennsylvania Legislature, by statute, chose to create only a duty of notice on the part of employers experiencing breaches. See id. at 1041 (citing Pennsylvania's Data Breach Act, 73 P.S. §§2301-2309). Clearly then, *Dittman* does recognize obligations on the part of Pennsylvania employers not embodied by prior Pennsylvania statute or case law.

The Legislative/Regulatory Approach

While *Dittman* is a harbinger for judicially-created obligations, it can hardly be considered an outlier for employers given that New York (and other states) have enacted or proposed regulations or statutes that require covered employers to assess, maintain and/or develop cybersecurity programs. New York, like Pennsylvania, has a statute requiring virtually all employers to provide written notice of a data breach involving certain types of PII to both affected individuals and the NYS Attorney General's Office, the NYS Division of State Police; and the Department of State's Division of Consumer Protection. See N.Y. Gen. Bus. Law §899-aa. New York regulations go much further. The Superintendent of Financial Services promulgated 23 NYCRR Part 500, a "first-in-the-nation" regulation establishing comprehensive cybersecurity requirements for certain banks, insurance companies, and other financial services institutions regulated by the New York Department of Financial Services (DFS). 899-aa regulations require covered employers to maintain a comprehensive "cybersecurity program designed to protect consumers' private data; a written policy or policies that are approved by the board or a senior officer; a Chief Information Security Officer [CISO] to help protect data and systems; and controls and plans to help ensure [] safety and soundness … ." See id. The DFS regulations impose periodic compliance, audit, reporting, and self-certification deadlines by covered entities' CISO.

The New York State Attorney General's office has also proposed Stop Hacks and Improve Electronic Data Security (SHIELD) Act. The proposed SHIELD legislation requires covered entities to maintain "reasonable safeguards to protect the security, confidentiality, and integrity of" certain PII, including but not limited to disposal of data. The proposed SHIELD legislation includes various examples of required technical, personnel-based, and physical cybersecurity measures. Importantly, the SHIELD legislation attempted to provide safe harbors for compliance with: (a) federal or state regulations or (b) a third-party assessors' certification, provided there is no evidence of willful misconduct, bad faith, or gross negligence.

> Without regard to who is making the legal rules, the change is upon us and certain practical steps will best serve the interests of both employers and employees in this digital era.

Pre-dating these cyber-specific legislative/regulatory efforts, §203-d of the New York Labor Law restricts the use of employee PII by all NY employers. Section 203-d prohibits New York employers from publicly posting or displaying an employee's Social Security number; visibly printing a SSN on an identification badge or card, including any time card; placing SSNs in files with open access; and communicating an employee's PII to the general public.

Notably, PII is defined as information "including an employee's Social Security number, home address or telephone number, personal electronic mail (e-mail) address, Internet identification name or password, parent's surname prior to marriage, or driver's license number." Most employers in NY protect SSNs, but many forget the requirements for home addresses, phone numbers, and driver's license numbers.

Violations of §203-d require proof of a "knowing" violation of the statute, and resulting fines up to $500. "Knowing" is not an employer-friendly standard and will be inferred if the employer has not adopted policies or procedures to safeguard against §203-d violations. Violations may be assessed where an employer lacks procedures to notify certain employees of these provisions. Proper training and education of employees is, therefore, a key safeguard against violations of §203-d. Indeed, many employers do not have procedures in place to limit access to employee PII to only those employees whose jobs actually require such access, typically a small percentage of the workforce.

Contrasting §203-d with the *Dittman* case, 899-aa and the proposed SHIELD legislation, it is clear that §203-d's provisions are limited to employee PII, whereas 899-aa and SHIELD encompass more robust protections for a greater range of PII, not just employee PII. Further, the limited scope of §203-d and the minimal penalties of $500 explain why 899-aa was enacted and SHIELD was proposed by NY's legislature with more comprehensive remedies.

The Preferred Approach

Dittman's common law approach of dealing with cybersecurity programs and data breaches leaves much to be desired. First, *Dittman* provides no guidance on what may be considered "adequate" or

"reasonable" cybersecurity measures for employee PII. Second, *Dittman* holds that the question of adequacy is essentially one of fact, inappropriate for resolution at the dispositive motion stage, likely answerable only after costly discovery (including, presumably, the cost of expert witness reports). Third, adequate compliance is left to second-guessing by plaintiffs' lawyers and trial judges who not only will likely lack the technical expertise to make such assessments, but may be asked to do so several months or even years after a breach takes place. Lastly, unlike the DFS regulations, *Dittman*'s broad strokes do not provide for safe harbors or exemptions for smaller employers.

New York's regulations are far from perfect. However, they do attempt to provide explicit guidelines for compliance, and a set of best practices and principles from which employers can proactively attempt to craft measures to protect employees' PII and mitigate the risk of breach events. Moreover, those regulations encourage periodic reassessment and independent audit of cybersecurity programs, together with mechanisms for employers to obtain periodic feedback from the regulators themselves. Other states' statutes, including Ohio, provide an affirmative defense against tort liability to companies who adequately comply with detailed cybersecurity regulations similar to those embodied in the DFS regulations and proposed SHIELD law. Thus, proactive legislative guidance would serve employees, employers, and the public much better than protracted ad hoc common law development of legal requirements.

What's an Employer to Do?

Cyberattacks and data breaches implicating employee PII are unlikely to go away anytime soon. Thus, regardless of jurisdiction or size, employers must recognize that the evolving legal landscape calls for action and self-evaluation. *Dittman* only underscores that cybersecurity obligations on employers are the new norm.

• **Assess the potential threat.** Start proactive compliance measures by assessing the process for collection and retention of current, prospective, and former employee PII. How much employee PII is the company taking in? Is it all necessary? How and where is the PII being stored after collection? For what length of time? Is that length of time consistent with the company's written retention schedules? Is that timing appropriate/necessary?

Cyberattacks and data breaches implicating employee PII are unlikely to go away anytime soon. Thus, regardless of jurisdiction or size, employers must recognize that the evolving legal landscape calls for action and self-evaluation. 'Dittman' only underscores that cybersecurity obligations on employers are the new norm.

• **Assess the safeguards.** In addition to assessing risk, employers should assess safety. Has the company adopted written security procedures to ensure protection of any stored PII? How comprehensive are the procedures? Are employees trained on the procedures? Have relevant stakeholders from legal, IT, and HR all been given an opportunity to weigh in on and propose changes to current security measures? Is someone responsible for periodic reassessment and review?

• **Conduct an audit of the safeguards.** Safeguards are only as good as the employees who follow them. Thus, it is important for employers to ask whether employees who have been trained on security procedures are following them? Do they understand the training they received? How often are employees being retrained and/or is the training itself being refreshed? How strong or vulnerable are technical procedural safeguards like encryption, firewalls, and authentication protocols? How often are independent audits of those safeguards being conducted?

• **Develop a plan.** Regardless of however strong the company's safeguards may be, it should be ready to confront a breach if it occurs. Does the company have an organized, step by step process to assess the scope of a potential breach? Is a written plan in place to ensure compliance with any state notification laws in the event of a breach? Has the company developed written risk-mitigation steps to implement post-breach in order to minimize the financial, legal, PR, employee relations, and other risks it may face post-breach?

• **Insurance.** Insurance can be a powerful financial risk mitigation tool to minimize the disruption and business impact of a data breach. Has the company purchased cyber insurance? Are the cyber policies broad enough to cover breaches of employee PII? Potential lawsuits arising out of same? Judgments? Legal fees?