PIERCE BAINBRIDGE BECK PRICE & HECHT LLP

boston | cleveland | new york | los angeles | washington, d.c.

MARCH 2019

PB Litigation SITREP[1]

Welcome to **PB Litigation SITREP**, Pierce Bainbridge Beck Price & Hecht LLP's monthly newsletter bringing you the latest news and insights on high-profile litigation and legal practice innovations that are rapidly changing the marketplace for lawyers and clients alike.

AREAS OF OPERATION: DATA PRIVACY

California Makes An Opening Bid for A National Privacy Standard

Consumers are increasingly encouraged to give businesses personally identifiable information ("PII") even as threats grow and cyberattacks become ubiquitous. Attention has focused on security and preventing data breaches, while the collection, storage, use, and sale of PII – the underlying asset – has received less attention. Scandals at technology companies, the Cambridge Analytica debacle in the 2016 U.S. presidential election, and the implementation of the Global Data Privacy Rule ("GDPR") have motivated legislators to consider enacting a national privacy standard that gives consumers the power to control the collection, use, and dissemination of PII.

While there is widespread acknowledgement that businesses need to be transparent regarding consumers' PII, Congress is unlikely to enact a national privacy standard until consensus emerges among stakeholders. Some core issues include:

• Concern that national privacy legislation will lack rigor compared to state laws and will deprive consumers of their private right of action to sue businesses regarding the collection, use, storage, and dissemination of PII;

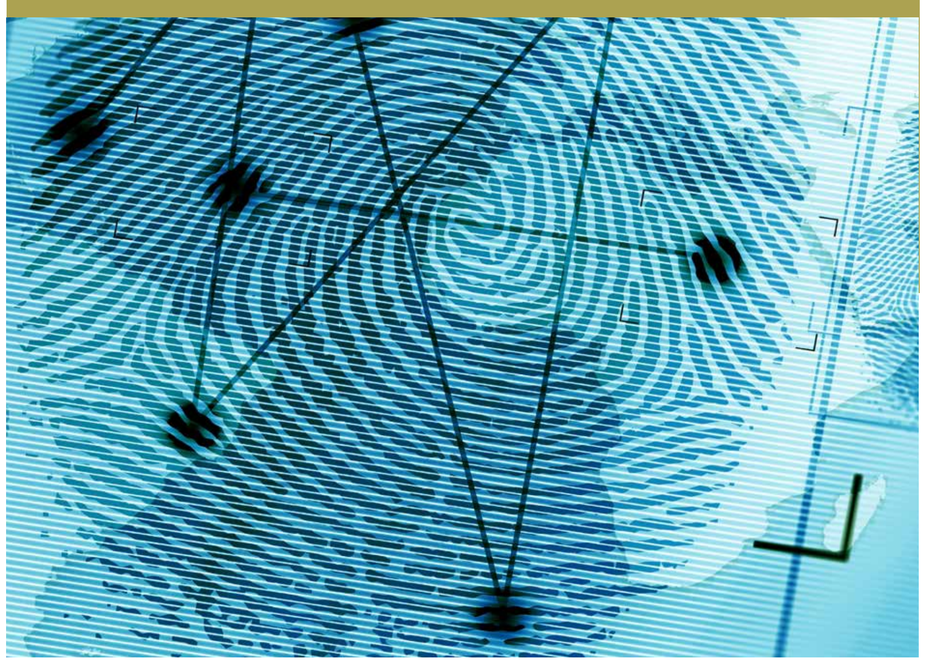
• Challenges in implementing a national privacy framework that is technology and sector agnostic and focuses on foreseeable risks that are likely to cause tangible consumer harm (the FTC standard) as opposed to prescriptive requirements;

• Uncertainty among lawmakers with respect to assigning a primary privacy regulatory and the structure of that regulator's enforcement regime across diverse industries.

Meanwhile, businesses will need to contend with a patchwork of potentially onerous state privacy laws, such as the California Consumer Privacy Act ("CCPA" or "Act"), which becomes effective January 1, 2020. The CCPA creates a costly near-term regulatory burden and other states will likely follow California's lead. Companies that act proactively can use a robust privacy governance program to gain a competitive advantage relative to peers, gain consumer loyalty, reduce consumer churn, mitigate litigation risk, and increase their bottom line.

The CCPA is the most far-reaching domestic privacy law, to date, and has been compared to GDPR because of its breadth and scope. Companies have until July 1, 2020 to become compliant before enforcement actions commence.

The Act applies to any "business" that collects "personal



information" of "consumers." "Business" means any for-profit company, that does business in California, collects the personal information of California residents and: (i) revenues exceeds $25 million annually regardless of where the revenue is earned; or (ii) buys, sells, or receives personal information of 50,000 or more California residents; or (iii) derives 50% or more of its annual revenues from the sale of California residents' PII. This includes affiliates that share similar branding. An out-of-state company is doing business in California if it actively engages in any transaction for the purpose of financial or pecuniary gain or profit in California. The Act exempts businesses that conduct all commercial activities outside California.

"Personal information" means "information that identifies, relates to, describes, or is capable of being associated, or could reasonably be linked, directly or indirectly, with a particular consumer or household." CCPA does not require an individual identifier (e.g., name, address, etc.) for PII to come within the statute.

"Consumer" refers to any "natural person who is a California resident ... however identified, including any unique identifier." Resident means "(1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary purpose," subject to certain specifications and clarifications.

These definitions reach many businesses because companies engage in "doing business" activities to access the State's 39.5 million residents, or employ California residents, either as full-time employees or independent contractors, via companies in the "gig" economy. Although smaller companies may escape the CCPA (most small businesses generate less than $25 million annually), many of them do business with regulated entities that the Act covers, and the regulated entities require vendors and service providers to have equally robust privacy policies.

Pierce Bainbridge deploys innovative technology and applies disruptive organizational principles to obtain the best litigation results for our clients. With offices in Boston, Cleveland, Los Angeles, New York, and Washington, DC, which are staffed by some of the market's most aggressive and talented litigators, and the ability to deploy legal talent to every corner of the world at a moment's notice, we have adopted the most current Digital Age concepts to win in both the courtroom and the boardroom.

[1] Military acronym for Situation Report.

CONTINUED

AREAS OF OPERATION: DATA PRIVACY

California Makes An Opening Bid for A National Privacy Standard

Consumers have three main rights under the CCPA: (i) the right to know; (ii) the opt-out right; and (iii) the right to delete PII except in certain circumstances.

Right to Know. Consumers have the right to know categories of PII businesses have collected, how PII was used, and the sale or dissemination of PII to third-parties. Prospectively, businesses must tell consumers, before any collection occurs, the categories of PII they will collect, and how the PII will be used. CCPA gives consumers the right to request *specific information* that a business has collected, the sources from which information was collected, and third-parties that received the PII. The look-back period is twelve months and businesses have 45 days to respond to a consumer's request.

Right to Opt-Out. Consumers have the right to opt out of the sale of their PII. Businesses cannot sell a consumer's PII once opt-out has occurred unless the consumer subsequently opts in and agrees to the sale of PII prospectively. Businesses must provide notice regarding the alternative to opt-out, and include a link on any websites stating, "Do Not Sell My Personal Information." Businesses must be alert to PII collected from minors, ages 13 – 16. Businesses cannot sell PII of a minor if it has "actual knowledge" that the consumer is under 16 years-old and it has not received specific authorization.

Right to Delete PII. Except for certain narrow exceptions, businesses must delete PII about a consumer if the consumer submits a verifiable request. Businesses must also notify its service providers of a consumer's request to delete PII.

The Act's non-discrimination rule buttresses these rights and prevents businesses from declining to provide services or goods because consumers exercise their privacy rights. A business may offer incentives to consumers for the collection, sale and non-deletion of PII. The incentives must directly relate to the value provided by the customer's PII.

Consumers have a private right of action when unencrypted or unredacted PII is stolen or disclosed because a business failed to maintain reasonable security procedures. Consumers can individually, or as a class, commence litigation to recover the greater of actual damages or up to $750 per incident, plus injunctive or declaratory relief, and other relief a court deems proper. Courts will look at factors such as the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, time during which misconduct occurred, willfulness of defendant's conduct, and the financial wherewithal of the defendant.

Consumers who seek relief because of an identifiable violation of the CCPA must notify the business prior to commencing litigation, either individually or as a class, and the business must provide the consumer a written statement within 30 days that it has cured the violation and that no further violation shall occur to avoid individual or class-wide statutory damages. Consumers can sue for breach of the written statement and statutory damages if the business fails to cure the statutory violation. Also, the Attorney General can bring a civil enforcement proceeding seeking an injunction for violation of the CCPA and monetary penalties up to $2,500 per violation of the Act and up to $7,500 for each intentional violation.

The CCPA will likely impact the business model of most business that use digital information. Yet, most companies

are unprepared for the CCPA regardless of industry. A PwC survey in October 2018 of more than 300 executives at U.S. companies with revenues above $500 million found that more than 50% of businesses will not be CCPA compliant by January 2020.

Companies should consider the following actions now to expedite CCPA implementation:

• **C-Suite and Board Engagement.** Assign responsibility for compliance to a C-suite executive with reporting responsibility to the CEO and have the Board include privacy risk as a regular discussion item on its agenda.

• **Evaluate Business Model.** Analyze ways to monetize PII securely (e.g., pseudonymize or decouple information so that it does not qualify as PII but maintains commercial usefulness) and offer consumers incentives in exchange for PII.

• **Data Mapping.** Map data to identify and classify categories and sources of PII collected from consumers.

• **Implement Privacy By Design.** Develop a principles-based privacy regime that allows the business to be proactive rather than focused on isolated rules. A commitment to protecting PII could create a competitive advantage relative to peers, mitigate potential reputational damage and subsequent loss of revenue from lower consumer confidence caused by litigation, and reduce customer churn. Moreover, additional privacy legislation is likely and privacy by design will save the company money.

• **Build a Privacy Governance Program.** Aggregate information from business units that gather PII; identify and remediate gaps; build a consumer self-service model that handles access requests for PII (opt-out and affirmative consent requests for the sale of PII, deletion requests, etc.); create a process for accountability and on-going monitoring; and ensure a cybersecurity framework exists within the company to protect encrypted data at-rest and in-transit.

• **Develop a Compliant Mindset.** Consider the type of evidence necessary to substantiate compliance when designing procedures, privacy notices, and websites (e.g., response protocols from consumer requests, clear and understandable privacy notices, audit logs to track consumer communication and responses, process and workflow audits to ensure the CCPA policy is working, etc.).

• **Evaluate Contracts with Vendor and Service Providers.** Analyze contracts to ascertain compliance with CCPA and, where necessary, modify contracts with entities whom you share PII to ensure you are protected from liability.

PIERCE BAINBRIDGE BECK PRICE & HECHT LLP

boston | cleveland | new york | los angeles | washington, d.c.

MARCH 2019

DUST-OFF: APPELLATE

Justice Fourth Amendment Style

Last month, Pierce Bainbridge partner Tillman Breckenridge and a team of his students from the Appellate and Supreme Court Clinic at the William & Mary Law School submitted a brief to the United States Court of Appeals for the Eleventh Circuit on behalf of Christopher Cantu, the personal representative of Robert Lawrence who was shot and killed by a police officer in Dothan, Alabama.

This case arose out of an encounter at the City of Dothan's Animal Shelter between an on-duty officer and Lawrence. According to the complaint, after Lawrence attempted to drop off a stray dog but refused to provide identification, the officer followed him to the parking lot to take down his vehicle's tag number. The officer also requested assistance which soon arrived. After a back and forth exchange with Lawrence, the back-up officer attempted to arrest him. The situation quickly escalated into a struggle. The back-up officer ultimately pinned Lawrence against his vehicle and the on-duty officer attempted to tase him. Lawrence then managed to grab hold of the taser's barrel, and the on-duty officer drew her firearm and shot Lawrence in the abdomen without warning. He died at the scene. His girlfriend and three young children were present.

Cantu sued the on-duty officer alleging excessive force in violation of the Fourth Amendment. The district court granted the officer's motion for summary judgment on the basis of qualified immunity. On appeal, Breckenridge and the team have advanced two principal arguments on behalf of Lawrence. First, they assert that, under the totality of the circumstances, the officer violated Lawrence's clearly established Fourth Amendment right to be free of excessive force when she fatally shot him without warning; and as her conduct was objectively unreasonable, the district court erred in granting qualified immunity. Second, they assert that the officer is not entitled to state agent immunity. For more on this appeal, the Dothan Eagle has coverage at this **link**.

AREAS OF OPERATION: PATENT

Diagnostic Methods v. Methods of Treatment

The patentability of diagnostic methods versus methods of treatment has been a recent focus of the Federal Circuit and as discussed below, may be heard before the Supreme Court.

This issue arises where patent claims cover subject matter that touches on natural processes or phenomena. As the Supreme Court has observed," all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 71 (2012). In *Vanda Pharmaceuticals Inc. v. West-Ward Pharmaceuticals Int'l Ltd.*, 887 F.3d 1117 (Fed. Cir. 2018), and *Athena Diagnostics, Inc. v. Mayo Collaborative Servs., LLC*, 915 F.3d 743 (Fed. Cir. 2019), the Federal Circuit distinguished claims to methods of treating disease from diagnostic methods that merely involved observing the result of a natural phenomenon. As the *Athena* court explained "[c]laiming a natural cause of an ailment and well-known means of observing it is not eligible for patent because such a claim in effect only encompasses the natural law itself. But claiming a new treatment for an ailment, albeit using a natural law, is not claiming the natural law." *Athena* at 752–53.

While the impact of these decisions on the biomedical field is still playing out, West-Ward Pharmaceuticals' successor, Hikma Pharmaceuticals USA Inc., has filed a petition for certiorari with the Supreme Court seeking to overturn *Vanda Pharmaceuticals Inc. v. West-Ward Pharmaceuticals Int'l Ltd.* The Court recently sought the current views of the Solicitor General on the questions presented, which hints that the case may be heard. While the outcome is uncertain, any ruling from the Supreme Court will have a broad impact on the biomedical field.

Pierce Bainbridge partners Brian Slater and Conor McDonough will be leading a round table discussion on this and related issues for personalized medicine at the Life Sciences Patent Network meeting, on April 25th in Boston. More information on the roundtable can be found **here**.

STRIKE FORCE: LATERAL HIRES

Jonathan Kortmansky (Partner): Civil and white-collar whiz Jonathan joins us from Sullivan & Worcester. His busy practice focuses on securities, products liability, bankruptcy, and white-collar criminal defense in additional to general commercial litigation.

Joan Meyer (Partner): White-collar and investigations icon Joan joins us from Baker McKenzie. She focuses on domestic and international white-collar defense for companies involving anti-corruption, financial fraud, government contracting, securities and commodities violations and trade compliance matters, as well as in advising on corporate compliance and best practices.

Abbye Ognibene (Associate): Class action ace Abbye joins us from Lief Cabraser Heimann & Bernstein, and focuses primarily on plaintiffs' class action litigation. Abbye also worked as a law clerk to the team on one of the consolidated cases that led to the nationwide right to marry for same-sex couples.

W. Tyler Perry (Associate): Complex commercialist Tyler joins us from Simpson Thacher & Bartlett LLP. He has worked on a wide variety of complex corporate, commercial, and securities disputes in federal and state courts, as well as on arbitrations.

Franklin Velie (Partner): Trial titan Frank joins us from Sullivan & Worcester. He has tried over 50 jury and non-jury trials and arbitrations, and handles a broad range of commercial matters including securities, products liability, white-collar criminal defense, domestic and international arbitration, employment law, accountants' and auditors' liability, insurance and bankruptcy.

Susan Winkler (Partner): Health care fraud litigation luminary Susan has over 30 years of experience handling some of the most scientifically challenging, high-stakes health care cases involving a wide range of issues.

We'll keep you updated in the next issue of PB Litigation SITREP.