# ADDITIONAL DEVELOPMENTS—PRIVACY

## *PICHLER V. UNITE*

*446 F. Supp. 2d 353 (E.D. Pa. 2006)*

The United States District Court for the Eastern District of Pennsylvania ruled that the Union of Needletrades Industrial & Textile Employees AFL-CIO ("UNITE") had violated the Driver's Privacy Protection Act (DPPA) by recording the license plate numbers of vehicles in employee parking lots and using the numbers to obtain employees' names and addresses from state motor vehicle records, a method sometimes referred to as "tagging." On cross-motions for summary judgment, the court found UNITE liable and awarded statutory damages of $2,500 to each named plaintiff. As part of a unionization drive, UNITE recorded license plate numbers from vehicles in the parking lot of Cintas. UNITE used Westlaw and private investigators to match license plate information with employees' names and addresses.

The DPPA, 18 U.S.C. §§ 2721-2725, limits the release or use of personal information that State Departments of Motor Vehicles (DMVs) have on vehicle owners and sets civil penalties for violations. Section 2721(a)(1) of the DPPA forbids state officials from "knowingly disclos[ing] or otherwise mak[ing] available to any person or entity . . . personal information . . . about any individual obtained by the [DMV] in connection with a motor vehicle record." Section 2724 provides for a civil cause of action: "A person who knowingly obtains, discloses or uses personal information from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court."

The DPPA contains fourteen exceptions, and UNITE claimed two of them as a defense: the "litigation exception" and the "government entity exception." The former authorizes the use of personal information "in connection with any civil, criminal, administrative, or arbitral proceeding." The latter allows access "for use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of [a government agency] in carrying out its functions."

The court held that the litigation exception did not apply, because at the time of the Cintas campaign, UNITE was "finding" new claims, not investigating them within the meaning of the statute. UNITE also claimed the "acting on behalf of a government agency" exception, arguing it was "playing the role of a 'private attorney general' in eradicating discrimination at Cintas." The court ruled that UNITE did not qualify for this exception, because UNITE failed to show how any of its actions during the Cintas campaign were carried out on behalf of any government agency.

## *IMS HEALTH INC. V. AYOTTE*

*490 F. Supp. 2d 163 (D.N.H. 2007)*

In IMS Health, the United States District Court for the District of New Hampshire struck down on First Amendment grounds a New Hampshire statute, 2006 N.H. Laws § 328, that prohibited the transfer and use of prescriber-identifiable information for certain commercial purposes. Specifically, the court held: (1) that the plaintiffs' First Amendment challenge was proper because the challenged statute restricted protected speech, (2) that intermediate, as opposed to strict, scrutiny applied because the statute affected only commercial speech, and (3) that the statute did not survive intermediate scrutiny. It granted the plaintiffs' motion for declaratory relief and a permanent injunction.

In reaching its holding, the court relied on a New Hampshire state court's detailed factual findings. The plaintiffs were two data mining companies, IMS Health Inc. and Verispan, LLC., whose business entailed buying prescription drug information from pharmacies and other outlets throughout the United States, including New Hampshire. The companies then stripped the data to remove any patient-identifiable information, aggregated the data by prescriber (usually, by individual doctor), combined it with other publicly available sources, and sold or otherwise provided the complete package of information on doctors' prescription habits to third parties like pharmaceutical companies, researchers, and analysts. Pharmaceutical company clients of the plaintiffs used the data primarily for marketing purposes, including to help sales representatives better target and tailor promotional and educational pitches, known in the industry as the "detailing" of drugs, to particular doctors.

The court examined the statute and its legislative history, observing the New Hampshire state legislature's concern that "detailing and related practices violated physician and patient privacy and increased health care costs in the state. The court explained that the New Hampshire Senate had considered pharmaceutical industry-related testimony, including as to the impropriety in gifts and perks that pharmaceutical company representatives gave to doctors based on prescriber information gleaned from companies like the plaintiffs. According to the court, the state senate concluded that doctors prescribed fewer generics because detailing influenced them, which in turn raised healthcare costs. The court found that the legislation—the first of its kind in the United States—was enacted in part to reduce drug costs.

The statute provided that "records relative to prescription information containing patient-identifiable and prescriber-identifiable data shall not be licensed, transferred, used or sold…for any commercial purpose" with some exceptions, but expressly "includ[ing]…advertising, marketing, promotion, or any activity that could be used to influence" sales or prescriber behavior in New Hampshire." The statute went into effect in 2006, and the plaintiffs substantially complied with it.

IMS Health and Verispan challenged the statute on the grounds that it restricted First Amendment-protected free speech. The court agreed with the plaintiffs that the statute restricted protected commercial speech, by restricting both the disclosure of prescription information and later speech based on the information (the drug companies' sales and marketing efforts). The court held that the factual and scientific nature of the information was immaterial to free speech analysis.

Having established that the statute affected protected speech, the court next considered whether the speech impinged was commercial and therefore warranted intermediate

scrutiny rather than strict scrutiny under applicable First Amendment jurisprudence. The court held the statute's explicit application to only commercial use dispositive, such that intermediate scrutiny applied.

The court then applied the three-part framework for intermediate scrutiny that the Supreme Court laid out in *Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557 (1980). The *Central Hudson* test first asks whether the government actor defending a speech-restricting statute has identified a substantial government interest that the regulation supports. The New Hampshire Attorney General put forth three potential interests: promoting the privacy of prescribing doctors, promoting public health, and reducing health care costs. The court held that the statute did not address any substantial privacy interest, for prescribing doctors work in closely-regulated industry and therefore have diminished expectations of privacy. The court also distinguished cases recognizing a state's interest in protecting consumers, not trained professionals like doctors, from commercial solicitation.

As to the public health and care cost reduction rationales, the court proceeded past the *Central Hudson* test's first step—whether a substantial government interest exists—to a consideration of whether the challenged law directly advanced the government interest (Central Hudson step 2) and was not more restrictive than necessary to do so (step 3). It found fault in the chain of reasoning the legislature used to justify the law. The court held that the link from provision of prescriber-identifiable data, to the effect on detailing practices, to increase prescriptions of brand-name drugs, to eventual increased costs was too weak to qualify as "directly advancing" the proffered state interests.

## *MINNESOTA'S PLASTIC CARD SECURITY ACT*

*Minn. Stat. § 325.E64 (2007)*

In response to credit card data breaches, Minnesota enacted the Plastic Card Security Act ("the Act") imposing strict liability on merchants who retain a customer's credit or debit card security data. The law applies to all merchants accepting payments from Minnesota residents, regardless of the merchant's physical location. The Act is the first of its kind, and codifies a requirement of the Payment Card Industry Data Security Standard (PCI DSS).

Under the Act, merchants must not retain card security code data, PIN verification code numbers, or the full contents of any track of magnetic stripe data subsequent to the authorization of the transaction. In the case of PIN debit transactions, the data may be maintained a maximum of 48 hours. The Act's restrictions on data retention have been in force since August 1, 2007, while provisions authorizing liability take effect on August 1, 2008.

If a merchant retains data in violation of the Act, and a security breach occurs, the merchant may be held strictly liable for any resulting damages. The Act defines security breach as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." In addition, merchants are liable for breaches caused by their service providers. Financial institutions affected by the breach can recover from the merchant the costs of reasonable action undertaken to remedy the damage, including any payments by that financial institution to its cardholders, as a result of the breach.