St. John's Law Review

Volume 93
Number 1 *Volume 93, 2019, Number 1*

Article 6

It's Nothing Personal: Why Existing State Laws on Point-of-Sale Consumer Data Collection Should Be Replaced With a Federal Standard

Kate Mirino

IT'S NOTHING PERSONAL:

WHY EXISTING STATE LAWS ON POINT-OF-SALE CONSUMER DATA COLLECTION SHOULD BE REPLACED WITH A FEDERAL STANDARD

KATE MIRINO[†]

"Are you interested in signing up to receive exclusive offers and news about our products via email?" We almost all have fielded some variant of this question at the check-out counters of the retail stores we frequent. And it is no wonder that businesses continue to experiment with new methods of obtaining our email addresses—it has been forecasted that, by 2019, more than 246 billion emails will be exchanged around the world each day.[1] In 2018, the prevalence of email in our daily lives is already overwhelming, making it "one of the most profitable and effective" platforms out there for promotional messaging.[2] From a commercial standpoint, email—"the lifeblood of the Internet"—allows for expansion beyond the traditional bounds of advertising and helps businesses penetrate the broader worlds of consumers.[3]

Technological growth as rapid as that which has occurred in the digital space over the past several decades is almost certain to generate ambiguities across all areas of the law. Privacy, and information privacy in particular, is one field in which especially puzzling questions have arisen. Information privacy, as distinguished from decisional privacy—the focus in *Roe v. Wade*, for example—can be viewed "as the result of legal restrictions

[†] Articles Editor, *St. John's Law Review*; J.D., 2019, St. John's University School of Law; B.A., 2012, Boston College. Many thanks to Professor Jeff Sovern for his helpful guidance on this Note.

[1] *Email Statistics Report, 2015-2019*, THE RADICATI GROUP, INC. 3 (2015), https://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf (last visited June 21, 2019).

[2] JEANNIEY MULLEN & DAVID DANIELS, EMAIL MARKETING: AN HOUR A DAY 4 (2009).

[3] *Id.* at 5.

and other conditions, such as social norms, that govern the use, transfer, and processing of personal data."[4] In the United States, information privacy is a segmented body of law, made up of a disconnected set of sector-specific rules, which have been established by an unintended mix of "federal and state legislatures, agencies and courts, industry associations, individual companies, and market forces."[5] Other commentators similarly have described United States information privacy as "ad hoc,"[6] "patchwork,"[7] and "piecemeal,"[8] the oversight of which has been entrusted to "a hodgepodge" of uncoordinated actors.[9]

Much of today's uncertainty in this area stems from the challenges those actors have faced in adapting a core principle of information privacy law—namely, what has been dubbed "personal data,"[10] "personal information,"[11] or "personally identifying information ('PII')"[12]—to contemporary life. Because it is the "personal" quality of certain types of information that springs consumer rights,[13] a clear definition of what counts as "personal" is crucial to any law in this sphere. Traditionally defined as "information relating to an identifiable individual,"[14]

---

[4] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004).

[5] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 22–23 (2000).

[6] *Id.* at 3.

[7] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 904 (2009).

[8] Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1088 (2006) (reviewing DANIEL J. SOLOVE, THE DIGITAL PERSON: PRIVACY AND TECHNOLOGY IN THE INFORMATION AGE (2004)).

[9] Shaffer, *supra* note 5, at 26 (identifying such "[r]esponsible agencies" as "the Federal Trade Commission, the Office of Consumer Affairs, the Office of Management and Budget, the Office of the Comptroller of the Currency, the Social Security Administration, the Department of Health and Human Services, the Internal Revenue Service, the Federal Reserve Board, and the National Telecommunications and Information Administration"). "To date, these agencies do not coordinate their data privacy oversight." *Id.*

[10] *See, e.g.*, Schwartz, *supra* note 4, at 2058.

[11] *See, e.g.*, Éloïse Gratton, *If Personal Information is Privacy's Gatekeeper, Then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information*, 24 ALB. L.J. SCI. & TECH. 105, 110 (2014).

[12] *See, e.g.*, Nancy J. King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices*, 60 FED. COMM. L.J. 229, 239 (2008).

[13] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1824 (2011); *see also* Gratton, *supra* note 11, at 110.

[14] Gratton, *supra* note 11, at 112.

from a modern perspective, personal data is a much hazier concept, and no standard definition has been established in the United States.[15] In today's world, even "a few scraps" of anonymous data on the Internet can be enough to piece together someone's identity;[16] thus, as the development of technology continues to accelerate onward, some commentators suggest adherence to a definition of personal data that is more fluid and dependent upon continuing social advancements.[17]

One subset of information privacy law that has proven particularly murky in modern application is that which governs how private entities collect the personal information of consumers during in-store transactions. California's Song-Beverly Credit Card Act ("Song-Beverly" or the "Song-Beverly Act"), for example, which was enacted in 1971 to bolster consumer protections against credit card fraud and preserve data privacy, prohibits businesses from requesting or requiring that a customer provide personal identification information during the course of a credit card transaction, subject to limited exceptions.[18] Similar laws have been enacted in several other jurisdictions, and they each apply to varying categories of information, transactions, and conduct.[19] One element that is consistent among them, however, is that they all were passed before "the advent of modern electronic payment methods, online transactions, downloadable products and the Internet," rendering their application in today's retail atmosphere uncertain.[20] Judicial interpretation of these laws necessarily involves some gap filling, and often varies from one jurisdiction to the next, leaving consumers with inconsistent

---

[15] Schwartz & Solove, *supra* note 13, at 1816.

[16] Mark Bartholomew, *Intellectual Property's Lessons for Information Privacy*, 92 NEB. L. REV. 746, 747–48 (2014).

[17] *See, e.g.*, Schwartz & Solove, *supra* note 13, at 1818.

[18] CAL. CIV. CODE § 1747.08(a) (West 2018).

[19] *See* MASS. GEN. LAWS ANN. ch. 93, § 105 (West 2018); *see also* D.C. CODE ANN. § 47-3153 (West 2018); N.Y. GEN. BUS. LAW § 520-a (McKinney 2018); KAN. STAT. ANN. § 50-669a (West 2018); MD. CODE ANN., COM. LAW § 13-317 (West 2018); N.J. STAT. ANN. § 56:11-17 (West 2018); OR. REV. STAT. ANN. § 646A.214 (West 2018); 69 PA. STAT. AND CONS. STAT. ANN. § 2602 (West 2018); 6 R.I. GEN. LAWS ANN. § 6-13-16 (West 2018); WIS. STAT. ANN. § 423.401 (West 2018).

[20] Amy P. Lally & Catherine M. Valerio Barrad, *Today's Retailers are Fighting Yesterday's Privacy Laws*, LAW 360 (June 27, 2014, 11:21 AM), https://www.law360.com/articles/552220/today-s-retailers-are-fighting-yesterday-s-privacy-laws.

safeguards and businesses with scant guidance on how to maintain compliant practices.[21]

Accordingly, this Note proposes a contemporary-minded federal solution to preempt and standardize the various, outmoded state approaches in this field. Part I engages in a historical overview of the development of information privacy law in the United States. Part II provides a summary and comparison of the existing state rules at play. Part III discusses the negative consequences—both to consumers and to businesses—of inconsistent regulation in this area, and explains why a federal solution is necessary. Part IV outlines the parameters of the federal regulation proposed by this Note.

I. THE HISTORY OF INFORMATION PRIVACY LAW IN THE UNITED STATES

Dating as far back as the colonial era, the common law always protected "against eavesdropping" in the United States.[22] Later on, the passage of the Third, Fourth, and Fifth Amendments to the United States Constitution reflected the intent of the framers to exclude the government from certain private realms of the people:[23] the Third Amendment limits the government's freedom to quarter soldiers in private homes;[24] the Fourth Amendment protects the "persons, houses, papers, and effects" of individuals from "unreasonable searches and seizures";[25] and the Fifth Amendment provides that no "private property [shall] be taken for public use, without just compensation."[26]

The United States Supreme Court had an opportunity to explore information privacy law concepts as early as 1877, when it held that sealed letters and packages in the mail, as opposed to newspapers, magazines, and other items intentionally left open to inspection, could be "opened and examined only under . . . warrant."[27] The Court recognized that *those* rights of

---

[21] *See id.*

[22] Daniel J. Solove, *A Brief History of Information Privacy Law*, PROSKAUER ON PRIVACY 1–4 (2006), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2076&context=faculty_publications.

[23] *Id.* at 1-5.

[24] U.S. CONST. amend. III.

[25] U.S. CONST. amend. IV.

[26] U.S. CONST. amend. V.

[27] *Ex parte* Jackson, 96 U.S. 727, 732 (1877); *see also* Solove, *supra* note 22, at 1–7.

individuals—whatever their precise definition or scope—were "of far greater importance than the transportation of the mail."[28] And in the spirit of the Fourth Amendment, the Court noted that "[n]o law of Congress [could] place in the hands of [postal] officials . . . any authority to invade the secrecy of letters and . . . sealed packages in the mail."[29]

With the advent of telegraphic messages as a mode of communication technology, courts and legislators grappled with how to regulate them.[30] Tort privacy, as discussed by Samuel Warren and Louis Brandeis in their celebrated *Harvard Law Review* article, *The Right to Privacy*,[31] had some influence on early perceptions of information privacy law.[32] Even in simpler times, Warren and Brandeis recognized that the evolution of society and technology will require continual endorsement of new rights,[33] and they cited the intricacies of modern life as "hav[ing] rendered necessary some retreat from the world."[34] Reviewing thoroughly a person's right to decide whether and how extensively his feelings or thoughts could be made public, the commentators also mused, in a broader sense, that an individual must be able to control public access to "that which is *his*,"[35] to elect "to be let alone,"[36] and to enjoy "the right to [his] *personality*."[37]

Whereas the currency of personal information in the nineteenth century was rooted largely in its role in the exchange of gossip,[38] personal information has, in later years, come to harbor more substantial, sophisticated sources of value. Through the 1960s and 1970s, digital recordkeeping systems and data analysis methods began to facilitate unprecedented means of

---

[28] *Ex parte* Jackson, 96 U.S. at 732; *see also* Solove, *supra* note 22, at 1-7.

[29] *Ex parte* Jackson, 96 U.S. at 733; *see also* Solove, *supra* note 22, at 1-7.

[30] *See, e.g.*, *Ex parte* Brown, 72 Mo. 83, 90–91 (1880) ("[t]elegraphic messages are . . . of recent origin, and, therefore, the common law furnishes nothing but analogies for our guide."); *see also* Solove, *supra* note 22, at 1-7.

[31] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see also* Schwartz, *supra* note 7, at 907 ("Tort privacy's centrality to the law of information privacy has also waned over time.").

[32] Schwartz, *supra* note 7, at 907.

[33] Warren & Brandeis, *supra* note 31, at 193.

[34] *Id.* at 196.

[35] *Id.* at 199 (emphasis added).

[36] *Id.* at 205.

[37] *Id.* at 207 (emphasis added).

[38] *Id.* at 196.

identifying individuals from their personal information.[39] As a result, the concept of privacy law in the United States was finally expanded to include clear control over one's personal data. In 1984, Congress enacted the Cable Communications Policy Act, and made a significant breakthrough in "not only refer[ring] to PII, but also mak[ing] PII the trigger for the applicability of the law."[40]

The law's means of protecting individual control over one's personal data developed as "Fair Information Practices" (or "FIPs")—certain duties on processers of personal information that revolve around the following principles:

> (1) limits on information use; (2) limits on data collection, also termed data minimization; (3) limits on disclosure of personal information; (4) collection and use only of information that is accurate, relevant, and up-to-date (data quality principle); (5) notice, access, and correction rights for the individual; (6) the creation of processing systems that the concerned individual can understand (transparent processing systems); and (7) security for personal data.[41]

United States privacy law enforces FIPs through different sets of rules for public and private actors,[42] and in the private realm, unlike the omnibus regimes at play in other countries, rules in the United States are generally sector-specific.[43] Some observers opine that this evolutionary path has been the result of legislative "react[ion] to public scandals," and not of a proactive commitment to comprehensive privacy protection.[44] The Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM" or the "CAN-SPAM Act"), for example, governs email, specifically.[45] It identified as problematic the "rapid growth in the volume of unsolicited commercial [email]" received by consumers,[46] and noted that inconsistent state laws on the matter made it difficult for businesses to comply with all applicable standards.[47]

---

[39] *See* Gratton, *supra* note 11, at 110; *see also* Schwartz & Solove, *supra* note 13, at 1821. Before computers, to link data to a person, the data would almost always need to contain the person's name or likeness. *Id.*

[40] 47 U.S.C. § 605 (2012); Schwartz & Solove, *supra* note 13, at 1824.

[41] Schwartz, *supra* note 7, at 907–08.

[42] *See* Shaffer, *supra* note 5, at 24.

[43] *See* Richards, *supra* note 8, at 1088.

[44] Shaffer, *supra* note 5, at 25.

[45] *See* 15 U.S.C. § 7701 (2012).

[46] § 7701(a)(2).

[47] *See* § 7701(a)(11).

CAN-SPAM's response to the dilemma was a nationwide regulatory scheme prohibiting private entities from, among other things, gathering consumer email addresses "through improper means" or sending false or misleading information to consumers via email.[48]

California's Song-Beverly Act and other state laws in the point-of-sale data collection field all are focused on one very specific zone of conduct: the requesting and recording of consumers' personal data by merchants at the time of sale. The laws differ, however, in important respects, both textually and as judicially interpreted and applied. Thus, motives similar to the driving forces behind CAN-SPAM warrant a standardized, federal solution.

II. CALIFORNIA'S SONG-BEVERLY ACT AND OTHER STATE LAWS AT PLAY

Over a dozen United States jurisdictions have laws that restrict how commercial entities may collect the personal data of consumers at the point of sale.[49] In general, the laws prohibit businesses from requiring a customer to provide certain types of personal information as a condition to accepting the customer's credit card as payment.[50] Aside from this basic unifying premise, the laws vary significantly. The exceptions they itemize, for

---

[48] 15 U.S.C. §§ 7703(b)(2)(A)(i), 7704(a)(1) (2012). Other examples of federal, sector-specific information privacy laws include: the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6502 (2012), which governs how entities collect personal information from children online; the Financial Services Modernization Act (the "Gramm-Leach-Bliley Act"), 15 U.S.C. § 6801(b) (2012), which governs how financial institutions collect and protect the personal information of consumers; and the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1301 (2012) et seq., which governs how entities collect consumer health information.

[49] *See* Lally & Valerio Barrad, *supra* note 20.

[50] *See* CAL. CIV. CODE § 1747.08(a)(2) (West 2018); *see also* KAN. STAT. ANN. § 50-669a(a) (West 2018); MASS. GEN. LAWS ANN. ch. 93, § 105(a) (West 2018); N.Y. GEN. BUS. LAW § 520-a(3) (McKinney 2018); N.J. STAT. ANN. § 56:11-17 (West 2018); 69 PA. STAT. AND CONS. STAT. ANN. § 2602(a) (West 2018); 6 R.I. GEN. LAWS ANN. § 6-13-16(a) (West 2018); WIS. STAT. ANN. § 423.401(1) (West 2018); D.C. Code Ann. § 47-3153(a) (West 2018); MD. CODE ANN., COM. LAW § 13-317(a) (West 2018). In Oregon, while a business may require a credit or debit card holder to provide personal information, it may not record that information on a transaction form. *See* OR. REV. STAT. ANN. § 646A.214(1) (West 2018). In California and the District of Columbia, businesses may neither require nor request that a credit card holder provide certain personal information as a condition to accepting the credit card. *See* CAL. CIV. CODE § 1747.08(a)(2); D.C. Code Ann. § 47-3153(a).

example, are inconsistent.[51] Many designate "special purpose[s]," such as shipping, warranty, delivery, servicing, installation, or special orders, for which a business may request and record a customer's personal information.[52] Others permit a business to collect a customer's personal information if the business's credit card issuers will not complete the credit card transaction without it,[53] or if federal or state laws or contractual obligations require the business to collect it.[54] Still others have carved out exceptions for businesses that process credit card transactions by mailing settlement forms to designated bankcard centers,[55] and for various other sets of circumstances.[56]

Perhaps the most troublesome discrepancy among these statutes, however, is their lack of alignment on a clear understanding of what counts as personal identification information—the type of data springing each law's applicability to consumer transactions. The varying definitions that have

---

[51] *See* Lally & Valerio Barrad, *supra* note 20.

[52] *See* CAL. CIV. CODE § 1747.08(c) (West 2018); KAN. STAT. ANN. § 50-669a(c) (West 2018); N.Y. GEN. BUS. LAW § 520-a(3) (McKinney 2018); 69 PA. STAT. AND CONS. STAT. ANN. § 2602(a) (West 2018); 6 R.I. GEN. LAWS ANN. § 6-13-16(b) (West 2018); WIS. STAT. ANN. § 423.401(2) (West 2018); *see also* D.C. Code Ann. § 47-3153(b) (West 2018); MD. CODE ANN., COM. LAW § 13-317(b) (West 2018). New Jersey has no such "special purpose" exception. Massachusetts and Oregon do, so long as the customer provides the information for one of the enumerated special purposes voluntarily. *See* MASS. GEN. LAWS ANN. ch. 93, § 105(a) (West 2018); OR. REV. STAT. ANN. § 646A.214(2) (West 2018).

[53] KAN. STAT. ANN. § 50-669a(c) (West 2018); MASS. GEN. LAWS ANN. ch. 93, § 105(a) (West 2018); N.Y. GEN. BUS. LAW § 520-a(3) (McKinney 2018); N.J. STAT. ANN. § 56:11-17 (West 2018); 69 PA. STAT. AND CONS. STAT. ANN. § 2602(a) (West 2018); 6 R.I. GEN. LAWS ANN. § 6-13-16(a) (West 2018).

[54] CAL. CIV. CODE § 1747.08(c)(3)(A), (C) (West 2018); 69 PA. STAT. AND CONS. STAT. ANN. § 2602(a)(3) (West 2018).

[55] MD. CODE ANN., COM. LAW § 13-317(b)(3) (West 2018); N.Y. GEN. BUS. LAW § 520-a(3) (McKinney 2018); 69 PA. STAT. AND CONS. STAT. ANN. § 2602(a)(2) (West 2018); 6 R.I. GEN. LAWS ANN. § 6-13-16(b) (West 2018).

[56] *See, e.g.*, CAL. CIV. CODE § 1747.08(c)(1) (West 2018) (permitting businesses to collect personal information in connection with cash advance transactions, and permitting motor fuel retailers to collect ZIP codes solely to prevent fraud, theft, or identify theft); MASS. GEN. LAWS ANN. ch. 93, § 105(c)(1) (West 2018) (permitting businesses to collect credit card information where the card serves as a deposit to ensure payment if default, loss, or another similar event occurs); *see also* MD. CODE ANN., COM. LAW § 13-317(b)(2) (West 2018) (permitting businesses to collect personal information where the credit card issuer's authorization with respect to the customer's available credit is unnecessary to conclude the transaction); 6 R.I. GEN. LAWS ANN. § 6-13-16(b), (c) (permitting businesses to collect personal information if the customer provides it pursuant to the business's request, or where the credit card issuer must provide authorization as to the availability of credit to conclude the transaction); WIS. STAT. ANN. § 423.401(2)(a) (West 2018).

been adopted for this term are discussed categorically below and provide a useful backdrop to the problems identified by this Note.

A. Expansive Definitions of Personal Identification Information

The farthest reaching state statutory definitions of "personal identification information" appear in California's Song-Beverly Act[57] and in Kansas's state statute.[58] These laws define "personal identification information" as "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number."[59]

In California, the imprecision of this definition coupled with the complexities of modern retail environments have required a certain level of judicial extrapolation to set the exact parameters of this term.[60] In *Pineda v. Williams-Sonoma Stores, Inc.*, for example, the California Supreme Court focused on the broad reach of the word "concerning" in holding that a customer's ZIP code qualified as "personal identification information" under the Song-Beverly Act.[61] Because a customer's ZIP code identifies the area in which he or she lives, in the court's view, it plainly satisfies Song-Beverly's standard as "information *concerning* the cardholder."[62] In support of its decision, the court located in

---

[57] CAL. CIV. CODE § 1747.08(b) (West 2018). Song-Beverly was enacted in 1971 and amended in 1991, 1995, 2004, 2005, and 2011, but never to set forth a modern conceptualization of what counts as "personal identification information." CAL. CIV. CODE § 1747.08 (West 2018).

[58] KAN. STAT. ANN. § 50-669a(b) (West 2018). Kansas's statute was enacted in 1992, more than twenty-five years ago. KAN. STAT. ANN. § 50-669a (West 2018).

[59] CAL. CIV. CODE § 1747.08(b) (West 2018); KAN. STAT. ANN. § 50-669a(b) (West 2018).

[60] *See, e.g.*, Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612, 620 (Cal. 2011) (holding that a consumer's ZIP code constitutes "personal identification information" under the Song-Beverly Act). The California Supreme Court's decision in *Pineda* contradicted the decision in *Party City Corp. v. Superior Court*, where the California Court of Appeal for the Fourth District had held that ZIP codes fell beyond the scope of "personal identification information" under Song-Beverly. Party City Corp. v. Superior Court, 86 Cal. Rptr. 3d 721, 736 (Cal. Ct. App. 2008)*; see also* Florez v. Linens 'N Things, Inc., 133 Cal. Rptr. 2d 465, 470 (Cal. Ct. App. 2003) (holding that the Song-Beverly Act prohibits requests for personal identification information before the credit card transaction has ended, even if the consumer understood that providing her information was not required and proceeded to provide it voluntarily).

[61] *Pineda*, 246 P.3d at 616.

[62] CAL. CIV. CODE § 1747.08(b) (West 2018) (emphasis added); *Pineda*, 246 P.3d at 616. The court considered "immaterial" the fact "that such information *might also*

Song-Beverly's legislative history an intent "to provide robust consumer protections" by preventing commercial entities from requesting and recording personal identification information not required to complete the credit card transaction.[63]

The timing of a retail store's request for personal identification information has also proven relevant under California case law for purposes of determining liability under Song-Beverly. In *Harrold v. Levi Strauss & Co.*, the California Court of Appeal for the First District found that Levi Strauss & Co.'s practice of requesting a customer's email address *after* the conclusion of the credit card transaction did not run afoul of the Song-Beverly Act.[64] The court explained that a reasonable consumer would consider the transaction complete after having been handed the purchased merchandise and a receipt, at which point a request for personal identification information could not reasonably be interpreted as a condition to accepting the credit card as payment.[65] From the court's perspective, Song-Beverly was designed to prevent retailers from collecting personal identification information "under the mistaken impression the information is *required* to process a credit card transaction."[66] The act does not prohibit retailers from collecting personal identification information from consumers who provide it voluntarily and understand that it is not required.[67]

Similarly broad understandings of personal identification information can be found in the statutes at play in Massachusetts, New York, New Jersey, Pennsylvania, Rhode Island, and Wisconsin, which define it as information that includes, but is not limited to, a customer's address or telephone number.[68] In Massachusetts, as in California, judicial direction has been needed to help define the scope of the term. In *Tyler v. Michaels Stores, Inc.*, the Massachusetts Supreme Judicial Court

---

pertain to individuals other than the cardholder." *Pineda*, 246 P.3d at 617 (emphasis in original).

[63] *Pineda*, 246 P.3d at 620.

[64] 187 Cal. Rptr. 3d 347, 353 (2015). Levi Strauss & Co. assumed for the purposes of this appeal that an email address counted as "personal identification information" under Song-Beverly. *Id.* at 349.

[65] *Harrold*, 187 Cal. Rptr. 3d at 350.

[66] *Id.* at 351 (emphasis added).

[67] *Id.*

[68] MASS. GEN. LAWS ANN. ch. 93, § 105(a) (West 2018); N.J. STAT. ANN. § 56:11-17 (West 2018); N.Y. GEN. BUS. LAW § 520-a(3) (McKinney 2018); 69 PA. STAT. AND CONS. STAT. ANN. § 2602(a) (West 2018); 6 R.I. GEN. LAWS ANN. § 6-13-16(a) (West 2018); WIS. STAT. ANN. § 423.401(1) (West 2018).

held that ZIP codes fell within the statutory definition of "personal identification information," reasoning that together with the customer's name and other public data, ZIP codes can provide a business with the tools to determine the customer's address or telephone number, both of which are explicitly listed in the statute as examples of personal identification information.[69] The court found support for this reading in the statute's primary legislative goal: "to guard consumer privacy in credit card transactions."[70]

B. Restrictive Definitions of Personal Identification Information

Other jurisdictions have more narrowly limited their understandings of personal identification information. In Maryland and the District of Columbia for example, point-of-sale data collection statutes apply only to a customer's address or telephone number.[71] Arguably less ambiguous than their more expansive counterparts, this definition nonetheless has called for judicial analysis in the District of Columbia.

In *Hancock v. Urban Outfitters, Inc.*, the United States District Court for the District of Columbia held that a ZIP code alone is not an "address" within the meaning of the statute.[72] The court also noted that retailer Urban Outfitters, Inc., by recording ZIP codes in its point-of-sale register systems, did not record that information "on [a] credit card transaction form" in violation of the statute.[73] On appeal, however, the D.C. Circuit explained that the district court had missed the mark in failing to address whether the plaintiffs had standing to sue and instead "[dove] into the merits of [the] case."[74] Moreover, the court concluded that under Supreme Court jurisprudence, the plaintiffs did not in fact have standing, for they had failed to allege "any cognizable injury" resulting from disclosure of their

---

[69] Tyler v. Michaels Stores, Inc., 984 N.E.2d 737, 743–44 (2013).

[70] *Id.* at 742.

[71] MD. CODE ANN., COM. LAW § 13-317(a) (West 2018); D.C. Code Ann. § 47-3153(a) (West 2018).

[72] 32 F. Supp. 3d 26, 32 (D.C. Cir. 2014), *vacated and remanded for lack of standing*, 830 F.3d 511 (D.C. Cir. 2016) ("[A] ZIP code cannot be considered the 'address' of the 'cardholder' since a ZIP code, at best, merely indicates an area in which multiple addresses may be located.").

[73] *Hancock*, 32 F. Supp. 3d at 33, *vacated and remanded for lack of standing*, 830 F.3d 511.

[74] *Hancock*, 830 F.3d at 513.

ZIP codes.[75] The court made reference to the basic principle that legislative drafting "cannot erase" the standing requirements of Article III of the United States Constitution by affording plaintiffs a statutory right to sue in circumstances under which they "would not otherwise have standing."[76] Accordingly, the precise meaning of "address" (and of "telephone number") in the District of Columbia remains somewhat open to interpretation.

III. A CONTEMPORARY REGULATORY STANDARD IS NEEDED AT THE FEDERAL LEVEL

A. Inconsistent Regulation in this Sphere Is Especially Costly

1. Point-of-Sale Systems

Most retailers use a point-of-sale system tailored to their individual business needs, including what is essentially a personal computer at each point-of-sale location, linked with a server in the back office of that location, all operated centrally from the company's headquarters.[77] Businesses under common management generally incorporate the same point-of-sale systems in all their locations.[78] Point-of-sale systems in retail settings all work in substantially the same way, but their operating databases differ.[79] The most commonly used databases in the United States are provided by Microsoft and Oracle, but other options include systems provided by Linux and Apple.[80] Additional market complexities are attributable to preferences for different system features, such as operator language, from one retail establishment to the next.[81]

Modifications to point-of-sale systems and all their components are generally time-consuming, expensive, and

---

[75] *Id.* at 514 ("The complaint here does not get out of the starting gate.").

[76] *Id.* (quoting Spokeo v. Robins, 136 S. Ct. 1540, 1547–48 (2016) (internal quotation marks omitted)).

[77] *See* Alexander Polyakov, *The Vulnerabilities of a POS System*, FORBES (Sept. 17, 2017, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/09/27/the-vulnerabilities-of-a-pos-system/#619f2694b581.

[78] *See* Richard T. Ainsworth, *Sales Suppression: The International Dimension*, 65 AM. U. L. REV. 1241, 1262 (2016).

[79] *See id.* at 1242 & n.7 (citing *DB-Engines Ranking*, DB-ENGINES, https://db-engines.com/en/ranking (last visited May 17, 2016) ("[R]anking some 264 different database management systems or database engines that help run POS technology.")).

[80] *See id.* at 1243–44.

[81] *See id.* at 1244.

disruptive to businesses.[82] These changes may be necessary, however, when one state's point-of-sale data collection law changes or is interpreted by a court in that state as having a new or different meaning. Accordingly, the regulatory regime for point-of-sale data collection practices that the United States as a nation has accepted—one that continues to take a unique path in each state—is no longer workable.

2. Employee Training

State-specific standards also render necessary more comprehensive employee training programs, to include versions specially tailored for each jurisdiction in which a unique set of rules governs. And because these regulations continue to remain open to judicial interpretation, the point-of-sale data collection policies of commercial entities must be subject to continual reevaluation, modification, and reimplementation, as needed. These considerations demand substantially more time and expense from an employee training perspective than would a regime in which a single, standardized set of rules applied across all jurisdictions.

Moreover, time spent by the typical United States worker with a single employer is on the decline: "[t]he median number of years that wage and salary workers had been with their current employer was 4.2 years in January 2016, down from 4.6 years in January 2014."[83] In the private sector, the median tenure of employees was less than half that of public-sector employees.[84] Employees in service occupations "had the lowest median tenure (2.9 years),"[85] and employees in sales and related occupations

---

[82] *See, e.g.*, TA Operating LLC v. Comdata, Inc., No. 12954-CB, 2017 WL 3981138, at *11 (Del. Ch. Sept. 11, 2017) (describing how the party switching its point-of-sale system anticipated a timeline of "approximately two years, but it ultimately took three years and four months . . . for the [new] system to be fully deployed."); *see also* e2Interactive, Inc. v. Blackhawk Network, Inc., 2012 U.S. Dist. LEXIS 190240, at *24 (W.D. Wis. Jan. 17, 2012) (noting that workaround platforms often are selected by smaller businesses that decide they cannot bear the costs of "modify[ing] their point-of-sale (POS) systems"); Burger King Corp. v. Cabrera, No. 10-20480-Civ., 2010 WL 5834869, at *5 (S.D. Fla. Dec. 29, 2010), *report and recommendation adopted*, No. 10-20480-Civ., 2011 WL 677374 (S.D. Fla. Feb. 16, 2011) (deciding a dispute over whether franchisee's refusal to replace point-of-sale system gave rise to proper and lawful termination by franchisor of franchisee's franchise agreements).

[83] News Release, *Employee Tenure in 2016*, BUREAU OF LAB. STAT., 1 (Sept. 22, 2016), https://www.bls.gov/news.release/archives/tenure_09222016.pdf.

[84] *See id.* at 2.

[85] *Id.*

were not much higher, with a median tenure of only 3.1 years.[86] These factors necessitate further padding of the already sizable employee training budgets set by retailers in the United States,[87] to ensure that their increasingly temporary labor force remain thoroughly educated about point-of-sale data collection laws and how to comply with them. Instead, a standardized federal regime would eliminate the need for such nuanced, state-specific training policies and procedures.

B. Existing State Statutes Are Obsolete

The above-described state statutes that govern data collection at the point of sale all were enacted at least twenty-four years ago. A handful of them were amended more recently, but not to address the problems stemming from continued reliance on provisions whose legislative purposes could not have contemplated modern retail practices or contemporary forms of personal identification information.[88] As a result, courts are left to divine how the lawmakers of yesteryear would have intended these statutes to apply today.[89] Retail entities are left to formulate compliant business practices in the face of ambiguous regulation,[90] and consumers must live with inconsistent protection of their personal data.

As discussed above, "retrofitting statutes piecemeal" can produce undesirable outcomes, for example, by generating mixed judicial understandings of statutory terms like "address."[91] By way of illustration, whereas the California Supreme Court and the Massachusetts Supreme Judicial Court both found that a customer's ZIP code counted as an "address" and thus qualified as "personal identification information,"[92] the District Court for the District of Columbia viewed a ZIP code as a mere fragment of

---

[86] *Id.* at tbl.6.

[87] In 2016, large companies budgeted an average of $14.3 million each to employee training, midsize companies an average of $1.4 million each, and small companies an average of $376,251 each. *2016 Training Industry Report*, TRAININGMAG, 32 (2016), https://trainingmag.com/sites/default/files/images/Training_Industry_Report_2016.pdf.

[88] *See* Lally & Valerio Barrad, *supra* note 20 ("[T]he Song-Beverly Credit Card Act predates the advent of modern electronic payments, online transactions, downloadable products and the Internet . . . .").

[89] *See id.*

[90] *See id.*

[91] *Id.*

[92] Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612, 618 (Cal. 2011); Tyler v. Michaels Stores, Inc., 984 N.E.2d 737, 743 (2013).

an address, which therefore did not rise to the level of "personal identification information."[93] Such deviations from one jurisdiction to the next, and continued dependence on rules ever subject to judicial transformation, are burdensome realities for commercial entities seeking to maintain shrewd business practices without discounting the privacy rights of their customers.

Moreover, in those few jurisdictions in which courts have applied existing, outmoded statutes to contemporary retail practices (namely, California, Massachusetts, and the District of Columbia), the courts' rationales have relied in part on generic principles of statutory interpretation in the face of textual uncertainty.[94] As Columbia Law Professor Karl Llewellyn first pointed out, canons of statutory construction "readily can be used to cancel each other out," giving rise to doubts about their purported objectivity and value as "tools to constrain judges."[95] The findings of one study reveal that even at the United States Supreme Court level, canons of statutory construction do not appear to impact "the Justices' tendency to vote consistently with their ideological preferences, at least in divided-vote cases."[96] Another study shows that many canons simply are ignored altogether by lawmakers during the statutory drafting process.[97] Thus, while employing traditional principles of statutory interpretation can seem like a useful exercise, the results may turn out to be a sharper reflection of judicial philosophy than of legislative intent.

---

[93] *See* Hancock v. Urban Outfitters, Inc., 32 F. Supp. 3d 26, 32 (2014), *vacated and remanded for lack of standing*, Hancock v. Urban Outfitters, Inc., 830 F.3d 511 (2016); *see also* Lally & Valerio Barrad, *supra* note 20.

[94] *See, e.g.*, *Pineda*., 246 P.3d at 616 (looking to the words of the statute as the most reliable indicator of statutory intent); *see also id.* ("[W]e do not construe statutes in isolation, but rather read every statute 'with reference to the entire scheme of law of which it is part' so that the whole may be harmonized and retain effectiveness."); *id.* (resorting to the dictionary definition of the statutory term "concerning" as guidance for determining legislative intent); Tyler v. Michaels Stores, Inc., 984 N.E.2d 737, 740–41 (2013) (relying on the title of the statute in question as "useful guidance" for determining legislative intent).

[95] Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes Are to Be Construed*, 3 VAND. L. REV. 395, 401–06 (1950); Anita S. Krishnakumar, *Dueling Canons*, 65 DUKE L.J. 909, 912 (2016).

[96] *Krishnakumar, supra* note 95, at 914.

[97] *See* Abbe R. Gluck & Lisa Schultz Bressman, *Statutory Interpretation from the Inside—An Empirical Study of Congressional Drafting, Delegation, and the Canons: Part I*, 65 STAN. L. REV. 901, 907 (2013).

Fresh statutory drafting in the point-of-sale data collection sphere certainly would produce rules more attuned to modern retail practices than those enacted decades ago. In addition, drafting practices today might simply be better than they were in the past. As some commentators have observed, notable improvements in legislative procedures since the birth of Song-Beverly and its counterparts have "fundamentally altered" how Congress creates laws[98] and have resulted in the creation of legislation that is "more precise and detailed" than ever before.[99] The overall lawmaking process has been thoroughly revamped and modernized. Custom-made legislative software, for example, now equips drafters with bill templates and automatic formatting features to help maintain stylistic uniformity across documents.[100] In addition, the staff makeup of congressional committees has become highly specialized, such that committee members, who in the past would have worked on bills across a range of legal topics, now dedicate themselves to a single, specific pocket of the law.[101] These advances in the legislative process can hardly be neglected in the point-of-sale data collection space, where the existing laws are so critically in need of reinvention.[102]

Even assuming the state statutes currently in effect, as supplemented by any necessary judicial interpretation, do indeed approximate their would-be contemporary objectives, there are boundaries to tasking the judiciary with the regulation of consumer data privacy.[103] If courts were responsible for weighing fact-specific privacy interests "against the benefits of free data flows"—an intricate policy determination better left to the legislature—the resolution of information privacy questions would require abundant time and resources.[104] And because the

---

[98] Jarrod Shobe, *Intertemporal Statutory Interpretation and the Evolution of Legislative Drafting*, 114 COLUM. L. REV. 807, 816 (2014) (noting how the Legislative Reorganization Act of 1970 "paved the way for the modernization of legislative drafting").

[99] *See id.* at 813 ("Today, statutes are thoroughly researched and written by large groups of experts who are more aware of what courts and agencies are doing than ever before . . . .").

[100] *See id.* at 821.

[101] *See id.* at 845.

[102] To simply amend existing statutes after courts have opined on their meaning in new contexts would fail to provide sufficient direction to courts, consumers, and retailers as novel questions continue to arise. *See* Lally & Valerio Barrad, *supra* note 20. Accordingly, a federal statutory approach is the most sensible solution.

[103] *See* Shaffer, *supra* note 5, at 37.

[104] *Id.*

situations in which those questions could arise are "virtually infinite," judges simply would not be able to manage them all.[105] The data privacy field is also uniquely challenging due to the "informational asymmetry" that exists between consumers and the entities that collect their personal data, as well as the "behavioral tendencies [of consumers] to underestimate long-term risk."[106] These realities can cause laypersons to formulate incorrect beliefs and further reinforce this Note's proposal that these important decisions be entrusted to a well-informed legislature.

C. Counterargument: The States as Laboratories

As Supreme Court Justice Louis D. Brandeis famously observed in a 1932 dissenting opinion, the states bear a solemn duty to test out the answers to emerging social or economic questions, and stifling a state's exploratory spirit "may be fraught with serious consequences to the nation."[107] A major benefit of our federal system is that it allows for "a single courageous state" to act as a laboratory and to engage in valuable trial and error "without risk to the rest of the country."[108] The judicial branch may at times decide to terminate that process,[109] but as Justice Brandeis cautioned, it must do so prudently, "lest [the courts] erect [their] prejudices into legal principles."[110]

In the information privacy law universe, commentators have acknowledged the states' particularly meaningful role as laboratories.[111] States have, for example, "been the first to identify areas of regulatory significance and to take action,"[112] responded to difficult questions with "innovative approaches,"[113]

---

[105] *Id.*

[106] Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 220 (2012).

[107] New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

[108] *Id.*; *see also* Thomas W. Hazlett, *Is Federal Preemption Efficient in Cellular Phone Regulation?*, 56 FED. COMM. L.J. 155, 172 ("The United States is perceived as a federalist experiment due to its relatively heavy use of overlapping jurisdictions, from mosquito abatement districts to the U.S. Government.").

[109] *New State Ice Co.*, 285 U.S. at 311 (Brandeis, J., dissenting) ("[The Court] may strike down the statute which embodies [an experiment] on the ground that, in [the Court's] opinion, the measure is arbitrary, capricious, or unreasonable.").

[110] *Id.*

[111] *See, e.g.*, Schwartz, *supra* note 7, at 916.

[112] *Id.* at 917.

[113] *Id.*

and made possible "simultaneous experiment[ation] with different policies."[114] But the ultimate goal of state experimentation is to utilize the findings gathered to pinpoint the most effective, workable solution to a problem. With respect to Song-Beverly and its equivalents, the states have had an opportunity to experiment—one that now has spanned several decades—and the time has come for analysis of the findings gathered and "coherent policy implementation of the knowledge gained."[115]

There are, of course, circumstances under which individualized, state-by-state regulation is more appropriate than a nationwide rule—namely, when the regulated conduct is territorially confined and there are few "market spillovers."[116] In those cases, the benefits of locally tailored approaches might well outweigh the costs of forgoing or disturbing economies of scale.[117] On the other hand, federal standardization makes more sense when an approach that has generated efficiencies in one jurisdiction is likely to do so in others, rendering "[b]alkanization" unnecessary, wasteful, and bad for consumers.[118] When diverse, state-specific rules govern conduct that is substantially the same across the country, local legislative and regulatory bodies look to maximize the benefits to their own constituents, where possible, by "shifting costs" to other jurisdictions.[119] Moreover, even if one jurisdiction deems stringent regulation of a particular activity unjustifiably costly, and therefore forgoes it, national businesses nonetheless often decide to comply with the rules of the most restrictive states, imposing on all states, and on all consumers, their costs of doing so.[120] By contrast, consumers enjoy both direct and indirect advantages when regulations are consistent nationwide.[121] They

---

[114] *Id.* at 918.

[115] *Id.* at 932.

[116] Hazlett, *supra* note 108, at 156.

[117] *Id.* at 175. State-specific rules are generally more suitable "when local markets are relatively idiosyncratic, when the benefits of diverse rules are large relative to the costs of non-uniformity, [and] when the rules adopted in one state are largely contained within that jurisdiction." *Id.*

[118] *Id.* at 177 n.74.

[119] *Id.* at 180. "[I]f decentralization would lead to . . . inequitable outcomes across states, these services should be provided by the national government." *Id.* at 179.

[120] *Id.* at 181. "[F]irms adjust to diverse regulations by conforming to those rules that allow for the best aggregate operations." *Id.* at 182.

[121] *Id.* at 184.

benefit directly from "reduc[ed] information costs," as the rules they may choose to educate themselves about remain constant in all settings, and they benefit indirectly from commercial efficiencies that result in lower prices.[122]

Under that analysis, in the point-of-sale data collection space, a federal regulatory regime is most sensible.[123] The conduct being regulated is substantially the same nationwide, and across all retailers, because it revolves around one basic commercial goal: to leverage the ever-escalating value of personal identification information.[124] Whether used to formulate personalized advertisements based on the specific interests of consumers, or to provide information about consumer purchasing behaviors, the "commodification" of personal identification information is a growing trend in the United States,[125] and businesses are certain to continue experimenting with new ways of obtaining it. This Note proposes that uniformity in the regulation of its collection at the point of sale will boost actual compliance and generate commercial efficiencies, resulting in more consistent protection of data privacy[126] and benefitting consumers in the form of lower prices.

Moreover, in an increasingly mobile world, where residents of one state frequently travel to and make purchases in various other states, it is far more practical to establish a single set of rules that applies across all fifty states. This truth seemingly has been realized in the privacy regulations of other countries, for example, in Canada and the European Union,[127] where

---

[122] *Id.* Uniformity in food labeling regulation, as an example, led to greater "consumer awareness of the ingredients in food." *Id.*

[123] *See, e.g.*, Schwartz, *supra* note 7, at 904 ("A patchwork of information privacy laws now exists in the United States, and it is one with federal and state elements. In the view of [Bill] Gates and many others, it would be preferable to create a single federal law for the private sector that would impose uniform standards.").

[124] *See, e.g.*, Schwartz, *supra* note 4, at 2056–57 ("The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.").

[125] *Id.*

[126] "[P]olling data reveal that Americans are extremely concerned about privacy, both on and off the Internet." Schwartz & Solove, *supra* note 13, at 1815.

[127] The member countries of the European Union include: Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom. *European Union: EU member countries in brief*, EUROPA,

consumers enjoy "broad-based" protections of their privacy and personal information.[128] By contrast, direct marketing in the United States is not stringently regulated[129]—and not by any sweeping federal laws. While proponents of continued reliance on "market mechanisms" to protect consumer data privacy[130] argue that efficiencies in private activity are most readily achieved "when government regulation does not constrain entrepreneurial activity,"[131] this Note's proposed federal regulatory scheme for the point-of-sale data collection realm will nonetheless facilitate greater efficiencies than are possible under the existing framework of conflicting state laws.

IV. THE FEDERAL SOLUTION

A. Both a Ceiling and a Floor

Federal regulatory schemes can set a "floor"—"a minimum standard that states may exceed"[132]—or a "ceiling," which "preempt[s] state legislation with the effect of weakening existing state standards," as it does not permit more stringent state regulation above and beyond the federal rule.[133] In order to realize the above-described efficiencies, consumer returns, and other benefits, uniformity is key, and thus both a floor and a ceiling are necessary.[134] Business leaders in the United States

---

https://europa.eu/european-union/about-eu/countries/member-countries_en (last visited May 16, 2019). For now, the United Kingdom remains a full member of the European Union, but that may change as a result of Brexit. *Id.*

[128] King, *supra* note 12, at 238.

[129] *Id.* Several commentators argue that "the appropriate architecture" for digital privacy protection in the United States in "the information age" is one in which a federal actor oversees the compilation and use of personal data. Richards, *supra* note 8, at 1092.

[130] Shaffer, *supra* note 5, at 27 ("Because of the government's ad hoc approach to data privacy, U.S. regulation of the private sector largely depends on industry norms and individual company policies that are developed in reaction to market pressures.").

[131] *Id.*

[132] Schwartz, *supra* note 7, at 919–20 (referencing the Video Privacy Protection Act of 1988, the Wiretap Act, and the Gramm-Leach-Bliley Act).

[133] *Id.* at 920–21. The "meritorious aspects" of one federal law—FACTA—were realized through restricting the extent to which the states could decide to allow for more stringent consumer privacy protection in their own laws. *Id.* at 921.

[134] Having recognized that some states may have opted not to regulate in this space because privacy in personal identification information matters less to their citizens, this Note's proposed federal standard would be imposed on a take-it-or-leave-it basis, such that each state would need to either adopt it or refrain from regulating. Such an approach aims to respect the decisions of those states whose

have also weighed in to declare ceiling preemption imperative to their backing of and cooperation with "any comprehensive legislation" in this area.[135]

B. The Definition of "Personal Identification Information"

Because it is "[t]he fact that certain information is *personal*" that triggers consumer rights in this area,[136] the parameters of information privacy law, in general, and of point-of-sale data collection law, in particular, necessarily are determined by the "currently unstable category" of personal identification information.[137] In light of this reality, it is difficult to understand how United States privacy law has not yet delineated a standard meaning for this term.[138] The need for one nevertheless remains exigent.

In the point-of-sale data collection sphere, a handful of existing state statutes indicate vague understandings of personal identification information as data "concerning" the customer,[139] and others simply provide non-exhaustive lists of what might qualify as personal identification information, like a customer's address or telephone number.[140] In other words, though assorted meanings have been ascribed to the term, "little thought" has been dedicated to why one makes more sense than others.[141]

This Note proposes doing away with a fixed definition of the types of data that are and are not within the scope of personal identification information, in favor of a more dynamic conceptualization of the term—one that accounts for the fact that technology "is constantly evolving," and that "depends upon changing technological developments."[142] Because the

---

citizens do not desire point-of-sale data collection regulations without sacrificing the benefits of maintaining uniformity across states whose citizens do wish to protect their privacy in these items.

[135] *See, e.g.*, *Microsoft's Bill Gates Wants New Privacy Law*, CIO (Mar. 8, 2007, 7:00 AM), https://www.cio.com/article/2441839/security-privacy/microsoft-s-bill-gates-wants-new-privacy-law.html; *see also* Elena Schneider, *Technology Companies Are Pressing Congress to Bolster Privacy Protections*, N.Y. TIMES (May 26, 2014), https://www.nytimes.com/2014/05/27/us/technology-firms-press-congress-to-tighten-privacy-law.html; Schwartz, *supra* note 7, at 921–22.

[136] Gratton, *supra* note 11, at 110.

[137] Schwartz & Solove, *supra* note 13, at 1816.

[138] *Id.*

[139] *See, e.g.*, CAL. CIV. CODE § 1747.08(b) (West 2018).

[140] *See, e.g.*, MASS. GEN. LAWS ANN. ch. 93, § 105(a) (West 2018).

[141] Schwartz & Solove, *supra* note 13, at 1827.

[142] *Id.* at 1818.

overwhelming goal of data collection at the point of sale is to forge new avenues of communication with consumers, the regulation addressing that conduct must set forth a definition of "personal identification information" that includes whichever mailboxes, physical or virtual, now known or later invented, at which a consumer might receive commercial marketing messaging. Such an approach allows for the inclusion of data like an individual's home address, telephone number, email address, Facebook username, Twitter handle, and Instagram account, all of which can be conceived of as, or serve as a pathway to, a consumer mailbox subject to potential targeting by advertisers. While articulating examples of these mailboxes is instructive, the broader definition remains "flexible and evolving," yet retains "coherent boundaries,"[143] such that the resulting body of data within the scope of the law is neither under- nor over-inclusive.[144]

C. Transaction Types Covered

The existing state statutes are limited, for the most part, to credit card transactions,[145] reflecting one of the legislative goals of their enactment—to minimize the risk of credit card fraud—but rather deserting the other goal of protecting consumer privacy. This Note proposes a rule that applies to all transactions at the point of sale, regardless of payment method, such that retailers are foreclosed from circumventing the spirit of the law by requesting and recording consumer mailbox information during transactions not covered by the regulation.

D. Mandatory Conduct

1. Informed Consent

Under this Note's proposed federal framework, merchants may record a customer's mailbox information only after informing the customer what it will be used for and notifying the

---

[143] *Id.* at 1827.

[144] *See* Gratton, *supra* note 11, at 113. In future contexts, the mailbox approach will likely still require some level of statutory interpretation. Having identified the challenges associated with judicial resolution of information privacy questions, this Note proposes delegation of that task to an administrative agency, such as the Federal Trade Commission, that is better equipped to manage it than is the judicial system.

[145] Some state statutes also apply to check payment transactions.

customer that providing it is voluntary and not required to complete the transaction.[146] The merchant must provide these notices in the same format—verbally or in writing—in which the request for the customer's mailbox information is made. The delivery of these notices must be sufficiently "clear and conspicuous" that a reasonable consumer would have an opportunity to absorb and understand them, free from unnecessary, distracting language.[147] Thus, whatever the merchant's objective in collecting a customer's mailbox information, it must be properly disclosed, allowing the customer to weigh the advantages and disadvantages of sharing that data and make an informed decision about whether to do so.

2. Employee Training

Under this proposed federal regime, merchants must establish company policies and procedures to ensure that any collected information is used only for those purposes for which the customer provided consent at the time of collection. The store associates directly involved in the compilation of consumer mailbox data must also be trained, initially and periodically throughout their employment, in accordance with those policies.[148]

CONCLUSION

Existing state laws in the United States that govern how businesses collect and record the personal identification information of consumers are relics from a time during which

---

[146] This architecture displaces the need to address the reality that "it is now possible to interpret almost any data as *personal information*." Gratton, *supra* note 11, at 113. Although sophisticated entities easily can "extrapolate a particular identity from a few scraps of online data," a merchant would be in violation of the proposed federal regulation if it used such an "extrapolated" identity without first having secured that customer's informed consent. Bartholomew, *supra* note 16, at 747.

[147] Lesley Fair, *Full Disclosure*, FTC (Sept. 23, 2014), https://www.ftc.gov/news-events/blogs/business-blog/2014/09/full-disclosure. The Federal Trade Commission's guidance on how to make effective disclosures—for example, by observing "[t]he 4Ps" (Prominence, Presentation, Placement, and Proximity)—would prove helpful in determining how to analyze whether a merchant's notice to a customer before collecting his mailbox information was sufficiently clear and conspicuous. *Id.*

[148] A business's good faith implementation of compliant policies and proper training of employees would serve as a safe harbor under this Note's proposed federal framework, such that one-off employee errors or single instances of non-compliance would not subject the business to potential liability.

lawmakers could not possibly have contemplated their application in modern retail settings. They also vary in important respects, for example, in their conceptualizations of what constitutes "personal identification information" and what activates consumer safeguards. These inconsistencies generate commercial inefficiencies, which harm consumers indirectly in the form of higher prices. Consumers also suffer more direct negative consequences as their data privacy remains subject to variable, impermanent protection across the country. Accordingly, a federal solution, with a design that contemplates modern retail goals and does away with unnecessary, ambiguous concepts, is needed to preempt and standardize the varying state regulations of these business activities.