SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Law Review

Volume 65 | Issue 3

2015

Problems at the Register: Retail Collection of Personal Information and the Data Breach

Glenn A. Blackmon

PROBLEMS AT THE REGISTER: RETAIL COLLECTION OF PERSONAL INFORMATION AND THE DATA BREACH

CONTENTS

INTRODUCTION 861
I. *CAPP V. NORDSTROM* AND THE SONG-BEVERLY CREDIT CARD ACT 862
A. *Robert Capp Allegations and the Song-Beverly Credit Card Act* 863
B. *Personal Identification Information and the Motion to Dismiss* 865
C. *Conditioning the Sale and Summary Judgment* 868
D. *The Evidence of Nordstrom's E-mail Capture Program* 870
II. MARKETING TOOL VS. DANGEROUS LIABILITY 871
A. *The Modern Retailer and the Benefits of Collection* 871
B. *E-mail Addresses, Reverse Appending, and the Information Retailers Obtain* 873
C. *"The Year of the Data Breach"* 875
III. PRIVACY AND RETAILER DISCLOSURE 877
CONCLUSION 880

INTRODUCTION

On December 21, 2012, Robert Capp entered a Nordstrom retail location in Roseville, California.[1] He picked out a couple items and then went to check out.[2] "In a ritual familiar to most shoppers," the cashier asked Mr. Capp for his e-mail address so that Nordstrom could send him the receipt for the transaction electronically.[3] Mr. Capp initially objected, but after some further prodding, he eventually gave the cashier his e-mail address, and the cashier entered it into Nordstrom's customer database.[4] If that had been the end of the interaction, Mr. Capp and Nordstrom would have gone their separate ways. However, Mr. Capp alleges that Nordstrom kept his e-mail ad-

1. Plaintiff Robert Capp's Response to Defendant Nordstrom, Inc.'s Statement of Undisputed Facts at 1, Capp v. Nordstrom, Inc., No. 2:13-cv-00660-MCE-AC (E.D. Cal. Oct. 30, 2013) [hereinafter Capp's Response].

2. *Id.*

3. Memorandum and Order at 2, *Capp*, No. 2:13-cv-00660-MCE-AC.

4. Capp's Response, *supra* note 1, at 2–3.

dress and began to send him promotional e-mails.[5] What happened next probably took Nordstrom by surprise and definitely raised questions about the collection of e-mail addresses at the register. Using an obscure California law called the Song-Beverly Credit Card Act,[6] Mr. Capp and a group of plaintiffs brought a class action complaint against Nordstrom for their alleged collection of Personal Identification Information at the cash register.[7]

Collection of personal information has become a common occurrence at the register. Using rewards programs and other information capture programs, retailers large and small now collect tremendous amounts of personal information from customers in order to directly market to them later.[8] Some may ask, "What is the big deal?" Giving up your e-mail or other pieces of personal data can't really hurt. Promotional e-mails are a minor inconvenience at best. Many people, however, do not realize what disclosure of even a small piece of personal information can actually reveal.[9] This rise in information collection has been followed by a parallel rise in the number of data breaches.[10] Retailers are collecting more information and not doing enough to protect it.[11] This Comment analyzes the collection of e-mail addresses and other personal information by retailers in the context of Robert Capp's case against Nordstrom. It balances the benefits with the security concerns and proposes a solution that at least partially protects consumers' interests.

I. *CAPP V. NORDSTROM* AND THE SONG-BEVERLY CREDIT CARD ACT

An e-mail address is a powerful marketing tool. It allows retailers to reach out to their customers directly with minimal intrusion. It is not surprising that retailers like Nordstrom aggressively seek out these e-mail addresses and market to them even more aggressively.[12] E-mail capture is now a normal facet of consumer life, and many customers reveal their e-mail addresses without giving it much thought. People have become accustomed to "the e-mail prompt." Unfortunately for

5. Complaint for Civil Penalties, Damages, and Injunctive Relief (Civil Code § 1747.08) at 5, *Capp*, No. 2:13-cv-00660-MCE-AC [hereinafter Complaint].

6. CAL. CIV. CODE § 1747 (West 2014).

7. Complaint, *supra* note 5, at 7–8.

8. *See infra* Part II.B.

9. *See infra* Part II.B.

10. *See infra* Part II.C.

11. *See infra* Part II.C.

12. *See infra* Part I.D.

Nordstrom, not all consumers appreciated its "Information Capture Policy."[13]

A. Robert Capp Allegations and the Song-Beverly Credit Card Act

Robert Capp's visit to a Nordstrom retail store was probably no different from millions of other visits during the 2012 holiday season. Mr. Capp walked into the Nordstrom location in Roseville, California, on December 21, 2012, to purchase a Christmas gift.[14] He picked up "two sweaters for [his] wife" and then went to check out.[15] Instead of going to a traditional register, a salesperson with a portable device called a mobile point of sale device ("MPOS") approached Mr. Capp and began to check out the two items he had chosen.[16] Although what exactly the salesperson said to Mr. Capp is in dispute, the salesperson rang up the two items, processed his credit card, and then asked Mr. Capp for his e-mail address so that Nordstrom could send him his receipt via e-mail.[17] Mr. Capp claims that he initially resisted this request but eventually gave it to the salesperson after she again asked him for the e-mail.[18] He then took his purchases and left the store.[19]

That likely would have been the end of the encounter, except that Nordstrom allegedly retained his e-mail address. According to Mr. Capp, Nordstrom began to send him "purely promotional emails on a nearly daily basis."[20] He also contends that Nordstrom used his e-mail address to "reverse append and obtain other additional personal identification information"[21] and that he "has received a more generalized increase in email traffic from retailers indicating that Defendant may have shared or sold his email address to others without his permission."[22] Instead of just deleting the promotional e-mails from Nordstrom, Mr. Capp and a group of plaintiffs decided to bring a civil suit against Nordstrom for the collection of their personal information.[23]

13. Complaint, *supra* note 5, at 2.

14. Capp's Response, *supra* note 1, at 1.

15. Nordstrom, Inc.'s Notice of Motion and Motion for Summary Judgment or, in the Alternative, for Partial Summary Judgment at 7, Capp v. Nordstrom, Inc., No. 2:13-CV-00660-MCE-AC (E.D. Cal. Oct. 9, 2013) [hereinafter Nordstrom's Motion for Summary Judgment].

16. Capp's Response, *supra* note 1, at 1.

17. Nordstrom's Motion for Summary Judgment, *supra* note 15, at 7–8.

18. *Id.* at 7–8.

19. *Id.*

20. Complaint, *supra* note 5, at 5.

21. *Id.*

22. *Id.*

23. *Id.* at 8.

The case centers on an old California privacy law: the Song-Beverly Credit Card Act.[24] The law was originally enacted in 1971 as a consumer protection statute.[25] "It made 'major changes in the law dealing with credit card practices by prescribing procedures for billing, billing errors, dissemination of false credit information, issuance and unauthorized use of credit cards.'"[26] The legislature then amended the statute in 1990 by including a new section addressing collection of personal information.[27] The legislature sought "'to address the misuse of personal identification information for, inter alia, marketing purposes, and [finding] that there would be no legitimate need to obtain such information from credit card customers if it was not necessary to the completion of the credit card transaction.'"[28]

The pertinent section of the statute makes it illegal for anyone

> that accepts credit cards for the transaction of business . . . [to] [r]equest, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the . . . corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise.[29]

The Act then further defines Personal Identification Information ("PII") 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."[30]

Capp's suit alleges that by requesting e-mail addresses to send e-mail receipts, Nordstrom illegally conditioned the credit card transaction on the receipt of personal information.[31] The collection might seem like a minor violation, but the statute provides for significant fines if Nordstrom is found liable. Under the code, a violator can be subjected to a civil penalty of $250 for the first violation and $1,000 for each subsequent violation.[32] If Nordstrom requested the e-mail ad-

24. CAL. CIV. CODE § 1747 (West 2009).

25. *Id.* § 1747.01.

26. Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612, 619 (Cal. 2011) (quoting Enrolled Bill Memorandum from Senator Alfred Song to Governor 1 (Oct. 12, 1971)).

27. *Id.*

28. *Id.* (quoting Absher v. AutoZone, Inc., 164 Cal. App. 4th 332, 345 (2008)).

29. CAL. CIV. CODE § 1747.08 (West Supp. 2015).

30. *Id.*

31. Complaint, *supra* note 5, at 7–8.

32. CAL. CIV. CODE § 1747.08(e) (West Supp. 2015).

dress of every customer that came into one of its stores, the potential penalty could be enormous.

B. Personal Identification Information and the Motion to Dismiss

With the civil penalties at stake, Nordstrom would have been wise to present a strong defense in their motion to dismiss. Their initial motion, however, completely missed the statutory argument. Instead of addressing the California law head-on, Nordstrom focused almost exclusively on preemption by federal statute.[33] It argued that the Controlling Assault of Non-Solicited Pornography and Marketing Act of 2003[34] ("Can-Spam"), a federal law that regulates commercial e-mail, "expressly preempt[ed] state laws regulating the collection and use of email addresses."[35] Only a single section even addressed whether an e-mail address constitutes personal identification information.[36] The district court was quick to notice the error. In an order to show cause, the court stated that the Defendant "essentially seeks an advisory opinion that a federal statute preempts a California statute—a California statute that Defendant contends does not apply."[37] The doctrine of constitutional avoidance requires federal courts to "avoid reaching a preemption issue if they can resolve the case on statutory grounds."[38] The court then ordered the Defendant to either show cause regarding why their motion to dismiss should not be denied or file a supplemental brief addressing this issue. Nordstrom chose the latter and submitted a new brief shortly thereafter.

Nordstrom's supplemental brief addressed the deficiencies of its earlier brief by adding several new arguments. Central to their new position was the contention that an e-mail address does not constitute

33. Notice of Motion and Motion to Dismiss Plaintiff's Complaint or, in the Alternative, to Strike Portions of Complaint; Memorandum of Points and Authorities at 4–9, Capp v. Nordstrom, Inc., No. 2:13-cv-00660-MCE-AC (E.D. Cal. Apr. 11, 2013) [hereinafter Motion to Dismiss Plaintiff's Complaint].

34. 15 U.S.C. §§ 7701–7713 (2012).

35. Motion to Dismiss Plaintiff's Complaint, *supra* note 33, at 1.

36. *Id.* at 8–9. "This motion addresses the preemptive effect of CAN-SPAM on Song-Beverly email marketing claims and does not address at this time the question of whether an email address indeed constitutes personal identification information under Section 1747.08. Nordstrom denies that an email address constitutes personal identification information." *Id.* at 4 n.2.

37. Order to Show Cause Why Defendant's Motion to Dismiss Should Not Be Denied as Not Properly Before the Court at 1, *Capp*, No. 2:13-cv-00660-MCE-AC.

38. *Id.* at 2.

personal identification information under the statute.[39] The Defendant argued that an e-mail address does not specifically "identify" a customer and that even though an e-mail address can be used to contact a customer, it does not "identify the area in which a person lives or is geographically located."[40] The Defendant further argued that excluding e-mails would be "consistent with the legislative history of the statute and the historical circumstances of the time."[41] The California legislature did not consider the Internet when it enacted either the initial statute or amended it.[42] Extending the statute to "requests for email addresses for the purpose of sending e-receipts would be pure speculation, which is not the proper role of the courts."[43] The Defendant then added a couple more minor arguments to rounds out its position.[44]

Unfortunately for the Defendant, even its new arguments could not save it from an adverse ruling. In a twenty-five-page order, the district court sided with the Plaintiff and denied the Defendant's motion to dismiss.[45] Citing heavily to a California Supreme Court case involving the retail collection of ZIP codes, the district court stated that "an email address is within the scope of the statute's 'broad term[s]' 'concerning the cardholder' as well because a cardholder's email address 'pertains to or regards to a cardholder' in a more specific and personal way than does a ZIP Code."[46] The court further stated that "[i]nstead of referring to the general area in which a cardholder lives or works, a cardholder's email address permits direct

39. Opening Supplemental Brief in Support of Motion to Dismiss Plaintiff's Complaint or, in the Alternative, to Strike Portions of Complaint at 3–8, *Capp*, No. 2:13-cv-00660-MCE-AC.

40. *Id.* at 5.

41. *Id.* at 8.

42. *Id.* at 9–10.

43. *Id.* at 10.

44. Specifically, Nordstrom argued that the collection of e-mail addresses fell under an exception to the statute that allowed PII to be collected if it is "'required for a special purpose incidental but related to the individual credit card transaction, including, but not limited to, information relating to shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders.'" *Id.* at 17 (quoting CAL. CIV. CODE § 1747.08(c)(4) (2014)). Nordstrom argues that collection for e-receipts qualified as a special purpose under the statute. *Id.* at 17–18. Finally, the Defendant argued briefly that application of the statute would violate its due process rights and constitute a First Amendment Violation. *Id.* at 15–17.

45. Memorandum and Order, *supra* note 3, at 25.

46. *Id.* at 11 (quoting Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612, 616 (Cal. 2011)).

contact and implicates the privacy interests of a cardholder."[47] The court noted that the "statute's overriding purpose . . . was to 'protect the personal privacy of consumers who pay for transactions with credit cards.'"[48] The court found that "'the Legislature intended to provide robust consumer protections by prohibiting retailers from soliciting and recording information about the cardholder that is unnecessary to the credit card transaction.'"[49] Nordstrom's "alleged conduct in this case—acquiring Plaintiff's email address for one reason, sending him a receipt, and then using the address for another reason, to send him promotional emails and to resell that information to other companies—directly implicates the purposes of the statute."[50]

With the main state law issue out of the way, the court held that the Plaintiff had met its initial factual burden[51] and addressed Nordstrom's preemption argument. The court analyzed the preemption language of CAN-SPAM[52] and determined that the Act was not preempted by federal law for two reasons. First, the federal law "preempts only state statutes that regulate the manner in which an email is actually transmitted and delivered ('use'), and the content of that email ('commercial messages'); whereas [the Act] . . . only regulates the request for the email address."[53] Second, the CAN-SPAM Act regulates "email messages" while the Act only applies to the "addresses" themselves.[54] The enforcement of one would not conflict with the enforcement of the other, and it would not be "'impossible for a private party to comply with both state and federal requirements."[55] In fact,

47. *Id.*

48. *Id.* at 9 (quoting *Pineda*, 246 P.3d at 619).

49. *Id.* at 12 (quoting *Pineda*, 246 P.3d at 620).

50. *Id.* The court specifically rejected defendant's narrow interpretation of the statute stating that a broad interpretation "is consistent with the rule that California 'courts should liberally construe remedial statutes in favor of their protective purpose, which, in the case of section 1747.08, includes addressing "the misuse of personal identification information for, inter alia, marketing purposes."'" *Id.* (citing *Pineda*, 246 P.3d at 617–18).

51. *See id.* at 16–17 (stating defendant had not shown that plaintiff failed to state a claim for which relief could be granted and reserving the factual issue of the reasonableness of plaintiff's belief that the credit card was required for further factual development).

52. "This chapter supersedes any statute . . . of a State that expressly regulates the use of electronic mail to send commercial messages." 15 U.S.C. § 7707(b) (2012).

53. Memorandum and Order, *supra* note 3, at 21.

54. *Id.*

55. *Id.* at 22 (quoting English v. Gen. Elec. Co., 496 U.S. 72, 79 (1990)).

the enforcement of the Act would "most likely have the effect of furthering the purpose of CAN SPAM."[56]

C. Conditioning the Sale and Summary Judgment

The case now stands ready for a ruling on summary judgment. The parties conducted limited discovery, and both sides have submitted multiple briefs in support and in opposition to their respective motions for summary judgment. The arguments boil down to three main issues: (1) Capp could not have reasonably believed that giving his e-mail address was required to complete the transaction; (2) collecting the e-mail address was a special purpose allowed under the statute; and (3) any collection qualifies as a bona fide error that absolves the company of liability.[57] The case, however, will likely hinge on the reasonability of the Plaintiff's belief that the e-receipt request was a condition of the sale.

A number of courts in California have recently considered the application of the statute to a request for personal information. In *Florez v. Linens 'N Things, Inc.*,[58] a California court of appeals considered a situation in which a retailer requested a customer's phone number before the transaction and then recorded that information as part of a "Telephone Capture Policy."[59] The court was forced to reconcile the "request" language of the statute with the requirement that a retailer condition the transaction on providing the information.[60] After considering the language of the statute, the court stated that a request should be reviewed from the "customer's standpoint," and "[w]hat does matter is whether a consumer would perceive the store's 'request' for information as a 'condition.'"[61] Applying this language to a similar case involving the collection of customer information for a "Reward Zone" enrollment program, the Central District of California held that a retailer could be held liable only if a "reasonable customer could perceive the request as a condition for the business's accepting the credit card."[62] The court then held that no reasonable customer would perceive the request to enroll in a customer loyalty program as

56. *Id.* at 23 (stating that "the number of email addresses available to companies that accept credit cards for the transaction of business will decline under the Credit Card Act" resulting in a general reduction of "unwanted commercial electronic mail").

57. *See* Nordstrom's Motion for Summary Judgment, *supra* note 15, at 20 (providing three main arguments for summary judgment).

58. Florez v. Linens 'N Things, Inc., 108 Cal. App. 4th 447 (2003).

59. *Id.* at 449.

60. *Id.* at 451.

61. *Id.* (emphasis omitted).

62. Gass v. Best Buy Co., 279 F.R.D. 561, 571 (C.D. Cal. 2012).

a requirement for completing the credit card sale.[63] A third court stated in an unreported decision that "it [is not] likely that a reasonable customer would perceive an offer to send a receipt by e-mail, made after the credit card has been approved and returned to the customer but before the receipt is printed, as imposing a 'condition' on using the credit card."[64] The court in that case only considered the request for PII in the context of class certification and did not rule on this specific issue.[65]

The question then falls to whether a reasonable customer would perceive Nordstrom's request for an e-mail address to send an e-receipt after the credit card transaction as a requirement to complete the sale. The Plaintiff contends the salesperson asked him multiple times to provide the e-mail address.[66] Initially, he denied the request, but after the salesperson allegedly said, "Well, we would rather email it to you," the Plaintiff said something to the effect of "[o]kay, [w]hatever."[67] In his deposition, he further stated that his "thought was, well, . . . it doesn't print . . . so I gave it to her."[68] He focused on the fact the he "reluctantly provided it" to the salesperson in order to complete the transaction.[69] On the other hand, Nordstrom argues that its employees were never trained to ask for a customer's e-mail more than once.[70] Even if they did, no reasonable customer would think that asking for an e-mail in order to send an e-receipt "was a condition of completing the purchase by credit card."[71] Whether a reasonable person would have found that the e-mail address was required is up for debate, and it is possible that the court could reject this "reasonable" standard.[72]

---

63. *Id.* at 572.

64. Gossoo v. Microsoft Corp., No. CV 13–2043 SVW, 2013 WL 5651271, at *4 (C.D. Cal. Oct. 9, 2013).

65. *Id.* at *2–4.

66. Plaintiff Robert Capp's Opposition to Defendant's Motion for Summary Judgment or, in the Alternative, for Partial Summary Judgment at 13, Capp v. Nordstrom, Inc., No. 2:13-cv-00660-MCE-AC (E.D. Cal. Oct. 30, 2014) [hereinafter Capp's Opposition].

67. Nordstrom's Motion for Summary Judgment, *supra* note 15, at 8.

68. Plaintiff Robert Capp's Reply to Defendant's Opposition to Plaintiff's Cross-Motion for Summary Judgment at 3, *Capp*, No. 2:13-CV-00660-MCE-AC [hereinafter Capp's Reply].

69. *Id.*

70. Nordstrom's Motion for Summary Judgment, *supra* note 15, at 13.

71. *Id.* (emphasis omitted).

72. The plaintiff actually contends that even though his belief was reasonable, it does not matter because the defendant violated the Act simply by requesting and recording personal identification, without more

D. The Evidence of Nordstrom's E-mail Capture Program

At this point, what is clear from the limited discovery is that Nordstrom realized the value of obtaining customer e-mail addresses and actively sought to obtain as many e-mail addresses as possible. In a document entitled "Spring Release 2011/e-receipt Phased Roll-out February 21-March 2," Nordstrom discussed the objectives of its e-mail receipts program.[73] The document notes that "[t]he most effective way of gathering and retaining new customers is through the corporate email marketing campaign."[74] It further states that an "[e]-receipt provides Nordstrom the opportunity to gain new marketing email addresses."[75] It also set progress goals for the program. At the time, Nordstrom had "marketable email addresses for 22% of all customers" and hoped to increase this by 2% in order to "generat[e] $5.5M in incremental revenue."[76]

Under the program, employees were encouraged to aggressively pursue the e-mail addresses of customers by phrasing the request as a statement, not a question. An internal e-mail among Nordstrom upper management states that employees "should be saying (not asking), 'What email address would you like your receipt sent to.'"[77] The e-mail address would then be entered into the system and would "auto-populate going forward when the credit card is used."[78] Nordstrom then instructs employees only to reveal the marketing purpose of the collection if the customer "is concerned they will receive too many emails from Nordstrom."[79] Store employees would also be reviewed based on their efforts to collect customer e-mail addresses.[80]

Although relatively few documents have emerged discussing the workings of Nordstrom's e-mail capture program, the documents de-

---

explanation, during a credit card transaction. *See* Capp's Reply, *supra* note 68, at 4.

73. Exhibit 5 to Declaration of James M. Lindsay, *Capp*, No. 2:13-cv-00660-MCE-AC.

74. Capp's Opposition, *supra* note 66, at 9.

75. *Id.*

76. *See id.* at 10.

77. Exhibit 7 to Declaration of James M. Lindsay, *Capp*, No. 2:13-cv-00660-MCE-AC.

78. *Id.*

79. Exhibit 8–9 to Declaration of James M. Lindsay, *Capp*, No. 2:13-CV-00660-MCE-AC.

80. *See id.* (outlining a review process for store and department managers "to coach store selling employees to use Mobile POS and E-Receipts to provide a better service experience for the customer"). The second page of the exhibit actually contains the percentages of e-receipt transactions that individual employees entered into. *Id.*

tailed above make it clear that Nordstrom placed a high value on collection of customer information. It seems like the program was relatively effective. The National Director of Service & Experience at Nordstrom, Lori Baldwin, revealed in a declaration for Nordstrom that around 30 percent of transactions at Nordstrom's stores result in the collection of a customer's e-mail address.[81] This reflects an almost 8 percent jump between 2011 and 2013.

II. MARKETING TOOL VS. DANGEROUS LIABILITY

The *Capp* case and the internal documents that have emerged highlight an ever-increasing trend in retailer collection and use of customer personal information.[82] Retailers have good reason to collect such information. E-mail addresses and other personal information allow retailers to better target their customers and can have a major effect on a retailer's bottom line. While technology allows retailers to collect, store, and utilize customer information, it also enables hackers to easily obtain large amounts of personal information about millions of people. Even something as simple as a lost e-mail address can have serious implications for a customer, and recent events show that retailers are no longer able to protect customer information.

A. The Modern Retailer and the Benefits of Collection

For more than a decade, retailers have been using various information capture programs in order to collect personal information and use it to better market to consumers.[83] And e-mail addresses are among the most valuable pieces of information. An e-mail address can provide a retailer with an extremely valuable way of increasing their own revenue, and the statistics back it up. At least "66% of consumers have made a purchase online as a result of an email marketing

81. *See* Declaration of Lorri Baldwin in Support of Nordstrom, Inc.'s Motion for Summary Judgment, or in the Alternative, Partial Summary Judgment at 5, *Capp*, No. 2:13-cv-00660-MCE-AC (stating that "more than 70% of purchase transactions at Nordstrom physical stores result in the customer receiving a printed receipt only").

82. Nordstrom stands at the forefront of this trend. *See* Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES, July 15, 2013, at A1. The retailer received a lot of criticism recently when it was revealed that "the company started testing new technology that allowed it to track customer's movements by following the Wi-Fi signals from their smartphones." *Id.*

83. *See* Florez v. Linens 'N Things, Inc. 108 Cal. App. 4th 447, 449 (2003) (describing how Linens 'N Things would collect information from customers). As far back as 2001, Linens 'N Things used a "Telephone Capture Policy" to obtain customer telephone numbers and then used software to fill in a profile about the customers. *Id.*

message,"[84] and in 2012 at least "44% of e-mail recipients made at least one purchase" as a result of an e-mail.[85] Retailers who sent marketing e-mails saw an average return of $44.25 for every $1 they spent on e-mail marketing.[86] Nordstrom's own internal documents back up these statistics. The same 2011 Release, referred to above, which advocated the importance of collecting e-mail addresses, noted that "the average customer spends $23 more a year when their [sic] email address is captured."[87] For every 2-percent rise in e-mail collection, Nordstrom expected to be able to market to 185,000 more customers and generate $5.5 million in additional revenue.[88] Taking advantage of an e-mail address could reap huge benefits for a retailer.

The e-mail address is just the start, though. Linking the e-mail address to other personal information and then coupling that information with purchasing habits can enable a retailer to specifically tailor advertisements to the individual customer and further increase the effectiveness of the information capture program. Target has been using analytics since the early 2000s and to great effect.[89] When a customer makes a purchase at a Target Store, it assigns them a unique ID number or "Guest ID."[90] Target then collects as much personal information about the customer as possible through its own stores and even by purchasing the information.[91] Then anytime "you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail [Target] sent you or visit [Target's] website, [Target will] record it and link it to your Guest ID."[92] The company then links the demographic information about

84. *See* Niti Shah, *18 Email Marketing Stats That'll Make You Better at Your Job*, HUBSPOT (Dec. 5, 2013, 2:00 PM), http://blog.hubspot.com/marketing/email-marketing-stats-list (citing Casey Hampsey, *Saturday Stat Series: The Influence of Email Marketing Messages*, DMA (Aug. 23, 2013), http://thedma.org/advance/data-driven-marketing-ideas/saturday-stat-series/).

85. Amanda Nelson, *25 Mindblowing Email Marketing Stats*, SALESFORCE BLOG (July 12, 2013), http://blogs.salesforce.com/company/2013/07/email-marketing-stats.html (citing Jay Baer, *15 Email Statistics That Are Shaping the Future*, CONVINCE & CONVERT http://www.convinceandconvert.com/convince-convert/15-email-statistics-that-are-shaping-the-future/ (last visited Mar. 23, 2015)).

86. *Id.*

87. Capp's Opposition, *supra* note 66, at 10.

88. *Id.*

89. Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, at MM30.

90. *Id.*

91. *Id.*

92. *Id.*

you to your spending habits and applies predictive analytics to decide what to market to you.[93] The program is so good at analyzing the data that it can predict when a customer is pregnant and then send them "an ad booklet, specifically designed for them."[94] The new system was so successful that "between 2002 . . . and 2010, Target's revenues grew from $44 billion to $67 billion."[95]

The implication of these data is clear. The industry has taken notice that the more information that a retailer can collect on its customers, the more profitable it can be. More and more retailers are collecting personal information in order to take advantage of this targeted marketing.

B. E-mail Addresses, Reverse Appending, and the Information Retailers Obtain

A ZIP code or even an e-mail address seems like just a small, insignificant piece of your identity. The problem lies in what an e-mail address means and what that and other small pieces of your information can reveal about you. Today, many people run their entire lives from their e-mail account. E-mail accounts today are linked to bank accounts and other financial institutions, health care providers, and other highly sensitive information. "A criminal can trawl through your emails and find a treasure trove of personal data: from banking to passport details, including your date of birth, all of which enables [identity] fraud."[96] Handing over an e-mail address gives a hacker one half of the "keys to your [virtual] kingdom."[97] A recent study by researchers at the University of Pittsburg demonstrated that "67.6% of participants use[d] their primary email addresses while

93. *Id.*

94. *Id.* ("Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There's, say, an 87 percent chance that she's pregnant and that her delivery date is sometime in late August. What's more, because of the data attached to her Guest ID number, Target knows how to trigger Jenny's habits. They know that if she receives a coupon via e-mail, it will most likely cue her to buy online. They know that if she receives an ad in the mail on Friday, she frequently uses it on a weekend trip to the store.").

95. *Id.*

96. James Silver, *20 Ways to Keep Your Internet Identity Safe from Hackers*, THE GUARDIAN (May 11, 2013, 19:01 EDT), http://www.theguardian.com/technology/2013/may/12/20-ways-keep-internet-identity-safe.

97. *Id.*

registering on other websites."[98] In many cases, these e-mail addresses were used as the actual "identity" of the person on these websites.[99] The problem with this is that "adversaries only need to compromise a user's primary account . . . in order to potentially compromise many of [the person's] other accounts on multiple websites."[100] Hackers who are able to compromise a weak password on an e-mail account can then use password recovery to crack into other online accounts, exposing a person's entire life to an identity thief.[101]

The retailers are not just limited to that one small piece of information either. For years, retailers have been asking consumers for one seemingly small piece of information then using that piece of information to fill in the blanks and create a complete profile. In *Florez v. Linens 'N Things*, the retailer asked the customer for a telephone number and then used "computer software that performs a reverse telephone search."[102] The retailer would then "[a]ssembl[e] the various pieces of the puzzle" to create "a record containing [a person's] name, credit card number, telephone number, and address."[103] The defendant in *Pineda v. Williams-Sonoma Stores*[104] used a similar process on customer ZIP codes to reverse append a customer's physical address, telephone number and e-mail address.[105] In *Capp*, the Plaintiff alleges that Nordstrom reverse appended his e-mail address to obtain other information about him.[106] A simple Google search for reverse appending of e-mail addresses reveals dozens of companies that claim to be able to do just that.[107] The reality is that even if a

98. Lei Jin, Hassan Takabi & James B.D. Joshi, *Security and Privacy Risks of Using E-mail Address as an Identity*, *in* SOCIALCOM 2010: IEEE INTERNATIONAL CONFERENCE ON SOCIAL COMPUTING 906, 908 (2010).

99. *Id.* at 906.

100. *Id.* at 909.

101. *Id.* It may be even easier for thieves to get into your account. A security firm called Hold Security recently discovered that a "Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses[.]" Nicole Perlroth & David Gelles, *Russian Hackers Steal Passwords of Billion Users*, N.Y. TIMES, Aug. 6, 2014, at A1.

102. Florez v. Linens 'N Things, Inc., 108 Cal. App. 4th 447, 449, 467 (2003).

103. *Id.*

104. Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612 (Cal. 2011).

105. *Id.* at 615.

106. Complaint, *supra* note 5, at 5.

107. *See Add Email Addresses to Your Contact Database*, TOWERD@TA, http://www.towerdata.com/email-append/email-appending (last visited Apr. 14, 2015) (offering to match names and addresses to e-mail addresses); *Postal Appending Overview*, FRESHADDRESS, http://www.

person gives just one small piece of personal information, a retailer can then go out and complete the story.[108]

C. "The Year of the Data Breach"

Since retailers have amassed so much information about their customers, it follows that they would go to great lengths to protect that information. The recent rash of data breaches, however, suggests that even some of the largest retail companies in the world either are not doing enough to protect consumer information or cannot combat the recent rise in hacking attacks. In a year that is being called the "year of the data breach," hackers broke into some of the largest companies in the United States and stole hundreds of millions of customer records.[109]

In December 2013, Target announced that hackers had broken through their security and spent two weeks stealing customer information.[110] The hackers installed "malicious software" on cash registers around the country and broke into millions of customer records.[111] By the time the hack was discovered and finally shut down, the hacker had stolen more than forty million credit and debit card numbers and seventy million customer records "that included the name, address,

freshaddress.com/services/postal-and-email-appending/postal-appending (last visited Apr. 14, 2015) (offering to match e-mail addresses to postal addresses); *Email Append and Reverse Append*, INFOGROUP TARGETING SOLUTIONS, http://www.infogrouptargeting.com/infogroup-targeting-solutions-digital-marketing/its-email-append-hygiene-services/email-append-reverse-append (last visited Feb. 21, 2015) (offering the same service).

108. With Target's capabilities, the "story" can actually be a frightening amount of information. A Target employee that was heavily involved in creating their analytical system stated that in addition to traditional information, Target can collect "your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet, and what websites you visit . . . your ethnicity, job history, the magazines you read, if you've ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own." Duhigg, *supra* note 89.

109. *60 Minutes: What Happens When You Swipe Your Card* (CBS News television broadcast Nov. 30, 2014), *available at* http://www.cbsnews.com/news/swiping-your-credit-card-and-hacking-and-cybercrime/.

110. Paul Ziobro & Danny Yadron, *Target Says Millions More at Risk—Probe of Computer Breach Finds Personal Data for 70 Million Exposed; Neiman Marcus Also Hacked*, WALL ST. J., Jan. 11, 2014, at B1.

111. *Id.*

email address and phone number of Target shoppers."[112] A leading watchdog on data breaches reported that between one and three million of these cards were sold on the black market, netting the hackers around $53 million and costing banks $200 million in card replacement fees.[113]

Then in April of 2014, a hacker broke into Home Depot's computer system through a "Pennsylvania-based refrigeration contractor's electronic billing account." [114] After gaining access, the hackers navigated the Home Depot system to steal customer information with a similar type of malware used in the Target breach.[115] Over the course of several months, the hackers stole nearly 56 million credit card accounts and approximately 53 million customer e-mail addresses.[116] The hack might have gone unnoticed had the hackers not posted some credit cards for sale online in September.[117] In a November press release, Home Depot specifically warned customers to look out for "phishing scams, which are designed to trick customers into providing personal information in response to phony emails."[118]

The hundreds of millions of records stolen from these two companies represent only the tip of the iceberg. Despite serious efforts to beef up security, "97 percent—*literally 97 percent of all companies*—are getting breached."[119] Often these companies do not even know they have been breached until "their customers' financial information goes up for sale in the underground [markets]."[120] Hackers can infiltrate and pilfer records from a system over long periods without detection. "On average the breaches from time of infection, from when the bad guys get in to the time they are discovered, is a

112. Brian Krebs, *The Target Breach, By the Numbers*, KREBSONSECURITY (May 6, 2014, 12:24 AM), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

113. *Id.* According to his website, Target also spent more than $100 million addressing the breach and saw a 46% drop in profits in the fourth quarter of 2013. *Id.*

114. Shelly Banjo, *Home Depot Hackers Stole Buyer Email Addresses*, WALL ST. J., Nov. 7, 2014, at A1.

115. *Id.*

116. *Id.*

117. *Id.*

118. Press Release, Home Depot, The Home Depot Reports Findings in Payment Data Breach Investigation (Nov. 6, 2014), *available at* https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

119. *60 Minutes: What Happens When You Swipe Your Card*, *supra* note 109 (emphasis added).

120. *Id.*

whopping 229 days."[121] What is clear from these breaches is that companies can never completely protect themselves from intrusion. "Even the strongest banks in the world—banks like JPMorgan, retailers like Home Depot, retailers like Target—can't spend enough money or hire enough people to solve this problem."[122] Really, all the retailers can do is try to control the damage.[123]

III. PRIVACY AND RETAILER DISCLOSURE

With hundreds of millions of customer records falling into the hands of hackers in the last year alone, it is clear that something needs to change. Retailers collect increasingly detailed records about their customers and then are powerless to stop hackers from taking it. Any solution needs to address how the retailers collect such information. There are a variety of federal laws governing how companies are supposed to use and protect customer information but none that govern how retailers collect such information at the register.[124]

State laws on the issue are not much better. There are a "patchwork" of states with laws that also prohibit the collection of personal information as a condition of accepting a credit card.[125] The laws in these states, however, are far from uniform and, like the Song-Beverly

121. *Id.*

122. *Id.* Ironically, while the hackers at Home Depot were "moving undetected into the company's systems in April, Home Depot was putting the finishing touches on a 45-page playbook on how to respond to a hack." Banjo, *supra* note 114.

123. "They're going to get in. But don't let them access the information that's really important. Don't let them get back out with that information. Detect it sooner. Respond sooner. And ultimately that exposure is very small." *60 Minutes: What Happens When You Swipe Your Card*, *supra* note 109.

124. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012) (governing how credit reporting agencies collect and use your information); Gramm Leach Bliley Act, 15 U.S.C. § 6801 (2012) (requiring financial institutions to safeguard sensitive consumer data). The FTC is empowered to bring cases against companies that do not protect customer data. FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2014 PRIVACY AND DATA SECURITY UPDATE, *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf. "Since 2002, the FTC has brought over 50 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk." *Id.* (emphasis omitted).

125. Martha C. White, *When a Retailer Asks, "Can I Have Your ZIP Code?" Just Say No*, TIME (July 11, 2013), http://business.time.com/2013/07/11/when-retailer-asks-can-i-have-your-zip-code-just-say-no/print/ (quoting Aaron Simpson, a partner specializing in privacy and cybersecurity at Hunton & Williams LLP).

Act, apply only to the collection of personal information in connection with a credit card transaction.[126] Any solution would have to come at the federal level and restrict the collection of personal information in any retail transaction.

The issue then becomes how to balance the benefits of collection of e-mail addresses and other personal information with the expanding privacy concerns. An outright ban would take away a valuable marketing tool and prevent consumers who might want to receive marketing materials from giving their information.[127] There is a middle ground though. In 2000, the Canadian Parliament enacted the Personal Information Protection and Electronic Documents Act[128] ("PIPEDA") in order to protect consumer personal information.[129]

126. *See* DEL. CODE ANN. tit. 11, § 914 (2007) ("write down or request to be written down the address and/or telephone number"); GA. CODE ANN. § 10-1-393.3 (2009) ("merchant shall be prohibited from requiring a purchaser to provide the purchaser's personal or business telephone number"); KAN. STAT. ANN. § 50-669a (2014) (writing down "personal identification information . . . including, but not limited to, the cardholder's address and telephone number"); MD. CODE ANN., COM. LAW § 13-317 (2014) ("may not record the address or telephone number"); MASS. GEN. LAWS ANN. ch. 93, § 105 (West 2006) ("write, cause to be written or require that a credit card holder write personal identification information"); MINN. STAT. ANN. § 325F.982 (West 2011) ("write down or request to be written down the address or telephone number"); NEV. REV. STAT. § 597.940 (2014) ("record a customer's telephone number"); N.J. STAT. ANN. § 56:11-17 (West 2012) (record "any personal identification information . . . including, but not limited to, the credit card holder's address or telephone number"); N.Y. GEN. BUS. LAW § 520-a (McKinney 2012) (require "any personal identification information, including but not limited to the credit or debit card holder's address or telephone number"); OHIO REV. CODE ANN. § 1349.17 (West 2004) (record "telephone number or social security account number"); OR. REV. STAT. § 646A.214 (2014) (may not write down "personal information"); 69 PA. CONS. STAT. ANN. § 2602 (West 2004) ("write or cause to be written . . . any personal identification information, including, but not limited to, the credit cardholder's address or telephone number"); R.I. GEN. LAWS § 6-13-16 (2014) (require to write "any personal identification information, including, but not limited to, the credit card holder's address or telephone number"); D.C. CODE § 47-3153 (LexisNexis 2012) ("request or record the address or telephone number"); WIS. STAT. § 423.401 (2014) ("record a customer's address, telephone number or any other identification information").

127. A retailer could always tell a customer to sign up online if they want to join an e-mail list or rewards program.

128. R.S.C. 2000, c. 5.

129. *Id.*; *see also* OFFICE OF THE INFO. & PRIVACY COMM'R FOR B.C., PRIVACY PROOFING YOUR RETAIL BUSINESS (2007), *available at* https://www.oipc.bc.ca/guidance-documents/1450 (outlining ten privacy principles: accountability; identifying purposes; consent; limited

With certain exceptions,[130] the law prohibits private organizations from collecting personal information "without the knowledge or consent of the individual."[131] PIPEDA then defines personal information broadly as "information about an identifiable individual."[132] Once an organization has collected personal information under the law, several other provisions go into action. The information may "only be used for the purposes for which it was collected," and the organization must adequately institute "appropriate safeguards," must not disclose the information, and must provide access to the information if a customer requests it.[133]

Such a law would go a long way toward protecting personal information in the United States. Companies would still be allowed to collect personal information and use it to market their products[134] but would have to specifically disclose how they are going to use the information.[135] Customers would then be able to make an informed decision about what information they would like to disclose to retailer. The customer would also have a civil cause of action if the retailer used it for secondary purpose. At the end of the day, it is really the consumer's responsibility to protect their personal information from dis-

collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance).

130. *See* R.S.C. 2000 c. 5, s. 7. (stating that a retailer can collect information without consent if "the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way . . . the information is publicly available and is specified by the regulations" and others).

131. *Id.*

132. *Id.* at 2.

133. OFFICE OF THE PRIVACY COMM'R OF CAN., PRIVACY TOOLKIT: A GUIDE FOR BUSINESSES AND ORGANIZATIONS 2 (2014) [hereinafter PRIVACY TOOLKIT].

134. *But c.f.* Exhibit 10-11 to Declaration of James M. Lindsay at 6, Capp v. Nordstrom, Inc., No. 2:13-cv-00660-MCE-AC (E.D. Cal. Oct. 30, 2014), ECF No. 36-14 (revealing the marketing purpose of the e-receipt program is "not effective").

135. PIPEDA requires a retailer to explain how it is going to use the information in a "clear, comprehensive, and easy to find" manner. PRIVACY TOOLKIT, *supra* note 133, at 12. Programs like Nordstrom's e-mail capture program would likely be illegal under the statute. A retailer may "[n]ever obtain consent by deceptive means." *Id.* "Under Canadian privacy laws, retailers using paperless receipt systems would have to let customers know about the way their emails will be used." Geoff Nixon, *Privacy Concerns Accompany Rise of Paperless Receipts*, CTV NEWS (Aug. 14, 2011, 8:48 PM), http://www.ctvnews.ca/privacy-concerns-accompany-rise-of-paperless-receipts-1.682558 (quoting Anne-Marie Hayden, director of communications for the Office of the Privacy Commissioner).

closure.[136] Consumers must be aware of what information they are giving to retailers and what surrendering that information means. A law requiring a retailer to disclose how they are going use that information would help a customer make that important decision.[137]

Conclusion

Robert Capp's suit against Nordstrom illustrates the means retailers are using to collect person information in order to better market their products. Collection of personal information is undoubtedly beneficial for a retailer's bottom line but can present a serious security risk to their customers. As the past year has shown, even the most technologically savvy retailers have been unable to protect such information. The United States should enact a broad statute governing the collection and use of personal information. A complete ban would be too restrictive, but requiring disclosure before collection would at least let customers know why their information is being collected and allow them to make an informed decision on what information they want to place in the hands of retailers.

Glenn A. Blackmon[†]

136. *See id.* (quoting Anne-Marie Hayden) ("Consumers, of course, also have a role to play. They should be aware of the implications of choosing an e-receipt over a paper one, and be prepared to ask questions of the merchant.").

137. The recent media storm over company data breaches has likely already had an effect on how consumers view their personal information. *See supra* Part II(C).

† J.D. Candidate, 2015, Case Western Reserve University School of Law; B.S., 2011, Business and Enterprise Management at Wake Forest University. Many thanks to Michelle Freeman and Jill McFarland for their guidance and feedback in creating and developing this Comment, the Law Review staff for all of their hard work, Erin Kampschmidt for putting up with my constant ramblings on the issue, and all the store clerks who asked for my e-mail in the last year.