

Protecting Privacy and Fostering Continued E-Commerce Growth

Eric Whisler – representing a coalition advocating for the retail industry

I. EXECUTIVE SUMMARY

The retail industry has a long history of balanced self-regulation to ensure that consumers' privacy is adequately protected, and industry best practices have evolved to timely meet privacy concerns created by online retailing. The current mix of regulation and industry self-regulation affords sufficient protection of consumer data collected in the online retail process.

Consideration of the retail industry's self-regulatory scheme, in light of the recently proposed FTC guidelines,¹ shows why new regulations are not necessary. The analysis will also show how the current proposal could potentially quash rapid growth in the e-commerce retail market and reduce customer utility. Regulations regarding notice, consumer choice, and changes to privacy promises should be flexible in order to properly handle various types and uses of information collected. Furthermore, regulation should focus on the use of information, such as sharing with third-parties, rather than the collection of such data.

Although we maintain that the current self-regulation regarding retailers' privacy practices is adequate, we also offer suggestions regarding the definition of behavioral advertising in case additional regulation is adopted. First, the definition should be narrowed to exclude first-party interactions with a website or websites affiliated through common ownership or control. Second, sensible exceptions should be made to account for different levels of trust and expectation inherent to existing customer relationships. Finally, the definition should be expanded to be technology and medium independent.

¹ FTC, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES, 2 (2007), <http://www.ftc.gov/os/2007/12/P859900stmt.pdf> [hereinafter FTC PROPOSED PRINCIPLES].

II. INTRODUCTION

As evidenced by the amount of economic activity attributable to the retail industry, the number of customers served, and the number of American workers employed, the United States retail industry represents a vital part of the economy. The most recent U.S. Department of Commerce E-Commerce Report shows that total retail trade sales—including both offline and online sales—totaled \$3.88 trillion in 2006.² One association member of our coalition, the Retail Industry Leaders Association (RILA), has over 200 members—including retailers, product manufactures, and service suppliers—representing combined annual sales in excess of \$1.5 trillion.³ These sales are made to the millions of American consumer RILA companies serve everyday in both traditional brick-and-mortar and online stores.⁴ Additionally, RILA companies employ millions of workers, and operate thousands of stores and facilities.⁵

The internet has quickly become a significant retail marketplace in which businesses connect with consumers.⁶ Online retail sales reached almost \$107 billion in 2006, and it is estimated that 2007 online retail sales totaled \$127.7 billion,⁷ Estimates for the first two quarters

² U.S. CENSUS BUREAU, U.S. DEP'T OF COMMERCE, 2006 E-COMMERCE MULTI-SECTOR REPORT Appendix Table 5 (2008) [hereinafter E-COMMERCE REPORT], available at <http://www.census.gov/eos/www/2006/2006reportfinal.pdf> and <http://www.census.gov/eos/www/2006/2006finaltables.pdf>.

³ Retail Industry Leaders Association, About Us-Overview, <http://www.rila.org/latest/rlAboutus.aspx> (last visited Nov. 11, 2008).

⁴ Letter from Katherine Luger, Senior Vice President, RILA to Donald Clark, Secretary, Federal Trade Commission 1 (Apr. 11, 2008), <http://www.ftc.gov/os/comments/behavioraladprinciples/080411rila.pdf> (regarding Online Behavioral Advertising Privacy Principles) [hereinafter *RILA Comments*].

⁵ *Id.*

⁶ Elizabeth Oesterle & Scott Silverman, *Comments of Shop.org, a Division of the National Retail Federation, and the National Retail Federation Before the Federal Trade Commission on "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles"* (April 11, 2008) <http://www.ftc.gov/os/comments/behavioraladprinciples/080411shoporgnrf.pdf> [hereinafter *Shop.org Comments*] (comparing the rapid growth in online retail sales to the 100 years it took catalog sales to reach a smaller percentage of total retail sales).

⁷ E-COMMERCE REPORT, *supra* note 2, at 3–4.

of 2008 reached \$68.2 billion.⁸ Although these totals represent a relatively small portion of total retail sales, 2.7 percent in 2006 and 3.2 percent in 2007,⁹ it is also important to consider the pace with which online retail sales have increased. Online retail sales experienced an average annual growth rate of 25.4 percent from 2001 to 2006, which far outpaced the 4.8 percent average growth in total retail sales.¹⁰ In sum, this data shows that the online retail industry accounts for an appreciable percentage of overall retail sales, and it is experiencing rapid growth.

One significant reason that the online retail industry is able to expand so quickly is because the internet provides retailers with instant feedback from their customers' shopping experiences. Online retailers have grown adept at harnessing the power of technology in their site redesigns, and they strive to provide new features that enhance the online shopping experience in ways traditional stores would never be able to provide. This is possible, in part, because the current regulatory and self-regulatory schemes allow companies to nimbly respond to customer preferences and technological change.

Our coalition of retailers believes the current mix of regulation and self-regulation appropriately allows retailers to create a competitive online retail marketplace through which consumer demand is satisfied while protecting their customers' privacy. Given the economic significance of the retail sector as a whole, and the current boom of online retail sales, any changes made to online privacy regulations should be carefully considered.

This paper will first provide a brief overview of data collected by typical retailers and provide examples of how such collection leads to enhanced customer utility. Next, it will describe the current self-regulation framework governing the retail industry in light of the

⁸ U.S. CENSUS BUREAU, U.S. DEP'T OF COMMERCE, QUARTERLY RETAIL E-COMMERCE SALES 2ND QUARTER 2008 Table 1, *available at* <http://www.census.gov/mrts/www/data/pdf/08Q2.pdf>. The quarterly report showed an estimate of \$33.6 billion for the first quarter and a preliminary estimate of \$34.6 billion for the second. *Id.*

⁹ *Id.*

¹⁰ E-COMMERCE REPORT, *supra* note 2, at 3.

recently proposed FTC self-regulation guidelines,¹¹ and explain why less extreme departures from the current regulatory regime are necessary to help ensure continued e-commerce retail growth. Finally it will encourage policy makers, if new behavioral advertising regulations are eventually adopted, to (1) clarify the definition of online behavioral advertising to exclude first party interactions; (2) provide exceptions based upon existing customer relationships; and (3) create regulations that are technology and medium neutral.

III. COLLECTION AND USE OF INFORMATION ON RETAIL WEB SITES

Data can be collected from and about retail customers in numerous contexts and for myriad purposes. Two general categories of information collected at a typical retailer site include (1) navigational or general browsing data—passively collected by the web server; and (2) user provided data—actively collected when the user deliberately enters information into a webpage form or dialog box.¹²

A typical retail website will gather navigational information during a visitor's use of its website. Information collected is generally non-personally identifiable information (non-PII), including a date and time stamp of the request, the user's browser type, service provider, referrer URL, and IP address.¹³ This information can inform the retailer about which pages of the website are most visited, provide information about technical efficiencies (such as the time it takes to download pages or fulfill requests), and help the retailer better understand a visitor's experience on the site.

The second type of data collected by a typical retailer is voluntarily provided by the visitor to its website, and may contain potentially personally identifiable information (PII). A

¹¹ See FTC PROPOSED PRINCIPLES, *supra* note 1.

¹² See PETER P. SWIRE & SOL BERMANN, INFORMATION PRIVACY: OFFICIAL REFERENCE FOR THE CERTIFIED INFORMATION PRIVACY PROFESSIONAL 203 (Peter Kosmala ed., 2007).

¹³ *Id.* at 215.

basic example of this is the store locator feature on a traditional brick-and-mortar retailer's website, through which address information is collected in order to identify the nearest store. Online retailers also collect electronic payment, billing, and shipping information to fulfill the order. Some of our retailers' websites have the ability to accept catalog requests, create a wish list, establish gift reminders, accept customer service requests, receive charitable donation requests, or accept employment applications. In each of these cases, the website visitor deliberately and voluntarily provides the information to the site.

It is worth noting that retailers have ample opportunity to collect potential PII offline as well and have been doing so for decades. Many of our retailers collect payment through credit cards and checks. Certain companies offer loyalty or discount cards, such as the popular grocery store cards, where customers provide contact and other information including mailing address, e-mail address, and phone numbers.¹⁴ Additionally, other companies may be legally required to collect personally identifiable information, such as during the sale of cold medicine which falls under laws intended to curb methamphetamine production.¹⁵

The combination of non-PII and PII data collected allows a retailer to improve its website by recognizing and delivering more of the products, services, and website features its visitors prefer. Our members contend that their customers have come to expect a streamlined shopping experience enhanced by the retailer's ability to store and quickly retrieve information related to the customer's past interactions with their website. This includes storage of payment information, addresses of gift recipients, persistent shopping carts, order history, order tracking, and facilitating returns. Some of the most successful online retailers have built reputations and a large client base because their websites offer personalized recommendations for a variety of

¹⁴ See, e.g., *RILA Comments*, *supra* note 4, at 1.

¹⁵ *Id.*

products based on a customer's prior orders or items viewed.¹⁶ Additionally, some successful online retailers are able to provide useful suggestions, reviews, and product comparisons based upon purchases made by others who have viewed or purchased a similar item.¹⁷ The ability to collect and analyze data collected through retail websites over time has improved the shopping experience for online retail customers and has allowed retailers to create more effective websites.¹⁸

IV. CURRENT ONLINE RETAIL SELF-REGULATION PRIVACY PROTECTIONS

Our member companies and associations have a history of promoting best practices regarding customer privacy through effective self-regulation in order to enhance customer trust and confidence in e-commerce.¹⁹ We also believe that when industry self-regulation is coupled with the already existing FTC enforcement mechanisms and FTC guidelines, consumer privacy is sufficiently protected in the online retail space.

One of our member associations, the Direct Marketing Association, Inc. (DMA), has been a leader in self-regulation regarding both offline and online privacy issues for decades.²⁰ DMA has a long track record of developing comprehensive self-regulatory guidelines which protect its customers' privacy online.²¹ Their members, and the members of our coalition, have a significant interest in ensuring the continued growth and success of e-commerce, and they understand that such success depends on their customers' confidence in the online marketplace.²²

¹⁶ Jerry Cerasale & Stuart P. Ingis, *Comments of the Direct Marketing Association, Inc. on Online Behavioral Advertising Proposed Principles*, (April 11, 2008) <http://www.ftc.gov/os/comments/behavioraladprinciples/080411dma.pdf> [hereinafter *DMA Comments*]

¹⁷ See *Shop.org Comments*, *supra* note 6, at 3.

¹⁸ *Id.* (noting research which found that retailers with an online presence of at least nine years were significantly more efficient at converting website visits to sales than retailers in the online business four years or less).

¹⁹ *DMA Comments*, *supra* note 16, at 4.

²⁰ *DMA Comments*, *supra* note 16, at 3.

²¹ *Id.*

²² *Id.*

The following discussion of the self-regulation guidelines promulgated by DMA²³ in light of the FTC's proposed online behavioral advertising principles will show that no additional regulation is necessary at this time in regards to online retailers.

A. *Transparency and Consumer Control*

At the core of the DMA online privacy guidelines are the notions of transparency and consumer control. Additionally, DMA strives to keep abreast of changing technology and consumer demands to determine how to best provide notice and build practices that empower consumers to make meaningful choices regarding the use of data collected while they shop online.

First, in regards to transparency, DMA guidelines require that retailers make their privacy policy available in a prominent place on their website's homepage, and make it "easy to find, read, and understand so that a visitor is able to comprehend the scope of the notice".²⁴ It is also required that the notice be available prior to or at the time PII is collected.²⁵ DMA members are also required to describe what type of PII may be collected, whether they use cookies or other passive means of data collection, and how such information may be used or shared.²⁶ In furtherance of the DMA transparency goals, they have developed tools to help their members provide consistent, clear, comprehensive, and comprehensible privacy policy disclosures.²⁷

²³ Direct Marketing Association, *Online Marketing Guidelines*, available at <http://www.the-dma.org/guidelines/onlineguidelines.shtml> [hereinafter *DMA Online Guidelines*]; Direct Marketing Association, *Guidelines for Ethical Business Practice*, available at <http://www.dmaresponsibility.org/Guidelines/> [hereinafter *DMA Ethical Guidelines*]

²⁴ *DMA Online Guidelines*, *supra* note 23.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *DMA Comments*, *supra* note 16, at 9–10. DMA provides its member companies access to privacy policy generation wizards through its website to help draft privacy notices which comport with existing regulatory schemes such as the Children's Online Privacy Act of 2000, the Gramm-Leach-Bliley Act, and the DMA guidelines. *Id.* at 10; *see also* <http://www.dmaresponsibility.org/PPG/>.

Second, in regards to honoring consumer choice, our coalition believes that a flexible approach is best, taking into account the nature of the information being collected and its potential uses.²⁸ We advocate that consumer choice does not need to be given at every point information is collected or used; this would be impractical. Such a stringent requirement could significantly hinder the online experience consumers have come to expect and negatively impact the efficiency with which our coalition members convert visits to their websites into sales.²⁹ However, the DMA requirements explicitly require member companies to offer and honor customer choice regarding the use of PII for marketing purposes, including both the use on the site where the PII was collected and the transfer of PII to third parties.³⁰

Although our coalition agrees with the notions of transparency in the FTC proposed principle, we take issue with its treatment of consumer control. In contrast to the flexible approach embodied in the DMA guidelines, the proposed FTC principle regarding control is too broad in scope and would constitute a major deviation from current public policy. First, the proposed principle seemingly covers collection of all “data” without regard to whether it is PII or non-PII. Requiring online retailers to change their e-commerce systems to accommodate choice regarding non-PII data could both hinder the evolution of the online marketplace by reducing the amount of information the companies use in analyzing customer behavior and impose significant re-design costs on the retailers. Second, shifting the focus from providing choice regarding *use* or *sharing* of information to choice regarding *collection* would deviate significantly from existing laws and public policy regarding privacy. One example is the Gramm-Leach-Bliley Act

²⁸ *DMA Comments, supra* note 16, at 10.

²⁹ *See Shop.org Comments, supra* note 6, at 9.

³⁰ *Id.* at 11. Article 31 of the *DMA Ethical Guidelines* require a retailer to allow existing and prospective customers to modify or eliminate direct marketing communications. *DMA Ethical Guidelines, supra* note 23. Additionally, Article 38 requires member retailers to notify customers if they transfer PII to third parties and provide an opt-out mechanism from such sharing. *Id.*

(GLBA), which focuses on the use and sharing of non-public personal information financial institutions obtain from their customers.³¹ The drastic shift in focus proposed by the FTC should not be adopted without identifying specific harms that justify forcing websites to provide opt-out for collection of any type of data. Nor should such a shift be adopted without thorough consideration of the potential impact on e-commerce as a whole.

B. Reasonable Security, and Limited Data Retention

Our coalition agrees that reasonable measures should be employed to protect consumer information stored by a member company. This is reflected in the DMA guidelines requiring companies to provide secured transactions and to protect databases containing PII against unauthorized access, alteration, or dissemination.³² We also agree that suggested factors to determine the reasonableness of protection include the sensitivity of the data, the nature of the company's business operations, the types of risks a company faces, and the reasonable protections available.³³ However, instead of considering data retention as a stand-alone category under a "legitimate business or law enforcement need" standard, we feel that it should be part of the overall reasonableness test for a data security program. Although legitimate business and law enforcement needs can inform a reasonableness analysis, they should not be the only considerations when determining how long it is appropriate for a company to retain customer data.

³¹ Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (1999); *see also* FTC, *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm> (last visited Nov. 12, 2008).

³² *DMA Online Guidelines*, *supra* note 23.

³³ FTC PROPOSED PRINCIPLES, *supra* note 1, at 4.

C. *Express Consent for Material Changes to Existing Privacy Promises*

Our coalition maintains that the current combination of FTC enforcement for unfair or deceptive practices and self-regulation are sufficient to appropriately handle material changes to an existing privacy policy. DMA guidelines regarding material changes to an existing privacy policy generally afford member companies flexibility in determining the appropriate notice and consent to give consumers after a material change. However, under current DMA guidelines, member companies must give consumers conspicuous notice of any material change with respect to sharing PII with third parties for marketing purposes and give them the opportunity to opt-out of the change.³⁴ Thus, DMA adopts a balanced approach which generally favors flexibility, but recognizes that certain situations demand a minimum response. The multifactor analysis advocated in DMA guidelines suggest that companies weigh the effect of the material change on things such as the type of customer relationship, the type of information at issue, the nature of the change, and the use of the information.³⁵ After thorough consideration of such factors members can determine what type of notice and choice is appropriate in order to ensure that their customers can continue to make informed choice about how information about them is collected, used, and shared.

The FTC proposed requirement of affirmative express consent for any material change is too broad, and could cause negative effects to both online consumers and to the overall e-commerce market. Although we agree that certain situations may merit opt-in treatment of a material change, we maintain that such a strict standard is not appropriate for every material change in a privacy policy. First, ensuring receipt of notice of the change and acquiring affirmative consent can be difficult. Research by one coalition member association found that

³⁴ *DMA Online Guidelines*, *supra* note 23; *DMA Ethical Guidelines*, *supra* note 23, at 19 (Article 37 deals with information security).

³⁵ *DMA Comments*, *supra* note 16, at 14.

only an average of 22 percent of emails sent by retailers are ever opened, around 11 percent of the emails are ever clicked through, and only about only about 6 percent will make a purchase.³⁶ If these statistics are indicative of the percentage of a retailer's customers who will opt-in after every material change, it is plausible that a single material change could reduce a retailer's marketing list by over 90 percent. Second, such a drastic reduction in marketing lists could have the effect of stunting development of retailers' websites, to the detriment of their customers' shopping experience and the e-commerce retail market. Faced with the knowledge under an opt-out regime that they could be forced to stop utilizing such a large portion of their marketing information, companies would likely avoid adding new features or services to their site that would constitute a material change. Alternatively, companies may decide to draft vague and amorphous privacy policies which would not result in as many material changes at the expense of transparency.

V. IMPORTANT CONSIDERATIONS FOR NEW BEHAVIORAL ADVERTISING REGULATIONS

In addition to the concerns about the FTC proposal raised above, we offer the following suggestions based upon the provided definition of behavioral marketing. The FTC proposal defines behavioral marketing as:

[T]he tracking of a consumer's activities online—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to deliver advertising targeted to the individual consumer's interests.³⁷

This definition is deficient for both being overbroad—by sweeping into its purview first-party and existing customer marketing—and too limited in scope—by focusing solely on online activities. As a result we offer the following three suggestions. First, the proposed definition of behavioral advertising should be narrowed, or have an explicit exception added, to exclude first-

³⁶ *Shop.org Comments*, *supra* note 6, at 11.

³⁷ FTC PROPOSED PRINCIPLES, *supra* note 1, at 2.

party interactions with a website and affiliated websites. Second, exceptions should be made for cases of existing customer relationships. Finally, behavioral advertising regulations should not be restricted to online collection of data.

A. *First-Party Marketing and Information Sharing with Affiliates*

Our coalition believes that the definition of behavioral marketing should not include practices at a single website or family of websites.³⁸ Under the proposed definition, regulations would apply to first-party marketing relationships between retailers and their customers, and they would treat information shared between a family of websites as if they are third-parties. These problems should be remedied by either narrowing the definition of behavioral advertising or explicitly adding an exception for at least two reasons.

First, without the exception or more narrow definition of behavioral advertising, the regulation could excessively interfere with the direct relationships that retailers have cultivated with their customers. As described above, many successful websites have developed tools and services to enhance the online shopping experience.³⁹ We maintain that online retail customers have come to expect a personalized shopping experience, leveraging the data collected from their previous experiences with the website. Furthermore, when consumers register at a website, request to receive e-mail newsletters or special offers, or complete a transaction, they are consciously sharing information with the website. Under existing self-regulatory guidelines, a conspicuous and comprehensible notice regarding the website's privacy practices will be given. As a result, companies are subject to legal constraints in the form of enforcement actions for deceptive or unfair trade practices under Section 5 of the FTC Act, and companies are also

³⁸ *DMA Comments*, *supra* note 16, at 6.

³⁹ *See supra* Part III.

subject to sanctions through participation in self-regulatory programs.⁴⁰ Furthermore, additional constraints such as reputational, market, and self-interest will help ensure that privacy promises are honored.

Second, treating the sharing of information amongst affiliated websites the same as information shared with third-parties would be a marked change from the public policy espoused in Title V of the GLBA.⁴¹ As required by the GLBA, a financial institution's privacy policy must provide its customers the ability to opt-out from having their non-public personal information shared before it can be shared with non-affiliated companies for marketing.⁴² However the act allows companies to share virtually any information with affiliated companies.⁴³ Marketing across affiliated websites under common ownership or control is beneficial to customers because it exposes them to a wider variety of product and service offerings and has the potential for significant cost savings.⁴⁴ Absent a showing of why all information collected from online users for first-party and affiliated marketing should be afforded more protection than inherently sensitive financial data, such a drastic shift in policy should not be made.

B. *Existing Customer Relationships*

Under existing law and regulation, companies are free to collect and use information in order to market to their own customers. Any regulations adopted dealing with behavioral

⁴⁰ Direct Marketing Association, Inc., *Complaint Handling Procedures & How To File A Complaint*, available at <http://www.the-dma.org/guidelines/complaintprocedures.shtml> (describing the complaint resolution process including potential penalties such as censure, suspension or expulsion from membership, public reprimand, and notifying governmental authorities).

⁴¹ Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (1999).

⁴² SWIRE & BERMANN, *supra* note 12, at 43.

⁴³ *Id.*

⁴⁴ *DMA Comments*, *supra* note 16, at 7.

advertising should include a concept analogous to an “established business relationship”⁴⁵ contained in other marketing regulatory schemes covering telemarketing and faxes.⁴⁶ This concept recognizes that consumers who have chosen to do business with a particular website have affirmatively expressed a level of trust and comfort in regards to the treatment of collection and use of information. Sensible additions in this regard would allow for different levels of notice or choice. We are concerned that the FTC proposal has left out this important exception.

C. Technology and Medium Neutrality

Finally, any new regulations adopted should be technology and medium neutral. Our members believe that using information collected about its customers’ activities online to suggest other products which may be of interest is analogous to experiences offline where merchants at a retail store assist customers personally. Principles that discriminate against online collection of information would straddle the burgeoning e-commerce retail market. Without findings to justify such disparate treatment, we advocate an approach consistent with existing U.S. privacy laws such as the GBLA and the Fair Credit Reporting Act⁴⁷ which apply the same rules both online and offline.

VI. CONCLUSION

Online retail sales have experienced stunning annual growth over the last decade. This growth is due in large part to the instant feedback retailers receive from their customers’ shopping experiences, and the ease with which websites log information. Online customers have

⁴⁵ See, e.g., FTC Telemarketing Sales Rule, 16 C.F.R. § 310.2(n) (including under the definition both customers who had purchased, rented, or leased a product in the previous 18 months and prospective customers who has inquired about the sellers goods or services in the prior 3 months).

⁴⁶ See, e.g., Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101–08 (as amended); Do-Not-Call Implementation Act, 15 U.S.C. § 6151 (as amended and extended); Junk Fax Prevention Act of 2005, 47 U.S.C. § 227 (2005).

⁴⁷ Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (as amended in 2008).

come to expect a personalized and streamlined shopping experience enhanced by the retailer's ability to store pertinent information. At the same time, rapid growth in both raw sales and online retail innovations is also fueled by the current regulatory and self-regulatory scheme governing the retail industry. This scheme offers a flexible approach which balances business needs with customer desires regarding how collected information is used and stored. It is our position that current self-regulation is sufficient to protect consumers' privacy, and warn that the current proposed principles may inadvertently reduce customer utility and hamper e-commerce retail growth.

However, if new regulation regarding behavioral advertising is eventually adopted, we suggest the following attributes for the definition of behavioral advertising. First, first-party interactions with a website or affiliate websites should not be included. Second, the definition should acknowledge that existing customer relationships create different concerns regarding notice, choice, and changes to privacy policies than do relationships with prospective customers. Finally, it should apply equally regardless of the technology or medium used, rather than focus solely on online activity.