



Stephen M. Lacy
Chairman and CEO

T: 515-284-3000

August 22, 2012

Hon. Joe Barton, Chairman
2109 Rayburn House Office Building
Washington, DC 20515

Hon. Edward J. Markey, Chairman
2108 Rayburn House Office Building
Washington, DC 20515

Hon. Henry Waxman
2204 Rayburn House Office Building
Washington, DC 20515

Hon. Steve Chabot
2351 Rayburn House Office Building
Washington, DC 20515

Hon. G.K. Butterfield
2305 Rayburn House Office Building
Washington, DC 20515

Hon. Austin Scott
516 Cannon House Office Building
Washington, DC 20515

Hon. Bobby Rush
2268 Rayburn House Office Building
Washington, DC 20515

Hon. Jan Schakowsky
2367 Rayburn House Office Building
Washington, DC 20515

Dear Sirs and Madam:

On behalf of Meredith Corporation, this letter responds to the inquiries you directed to Meredith on July 25, 2012 relating to the practices of “data brokers.” Founded in 1902 as an agricultural publisher, Meredith has evolved into one of America’s largest media and marketing companies with operations in magazine publishing, television broadcasting, brand licensing, integrated marketing, interactive media, and video production. Meredith’s National Media Group publishes 21 subscription magazine titles and more than 150 news stand titles with a combined circulation of nearly 30 million readers. Our magazine portfolio focuses on the home and family market and includes iconic titles such as *Better Homes and Gardens*, *Family Circle*, *Ladies’ Home Journal*, *Parents*, *Fitness*, *American Baby*, *More* and *Traditional Home*. Our Local Media Group operates twelve network-affiliated television stations.

Both our national and local media divisions maintain an extensive Internet and mobile presence. Many of our magazine titles are distributed over digital platforms, including the Apple iPad, Barnes & Noble Nook and Amazon Kindle. Together, our national and local media properties operate more than 50 websites and mobile websites and nearly 50 mobile applications. Collectively, these digital properties deliver approximately 725 million page views to approximately 40 million unique visitors each month, including 2 million news clips viewed in near-broadcast quality.

Like most if not all of our peers in the media industry, Meredith collects and uses information about consumers primarily in its capacity as a media publisher and does so in the context of a direct relationship to the consumer. Like other publishers, we use this information primarily to help us understand and engage our audience, improve our products, personalize and tailor content to audience interests, increase our circulation and deliver and target advertisements in our publications and digital properties, including websites and apps. Our production of high-quality editorial content, particularly digital content which we distribute for free or at low cost—is predominantly supported by advertising revenues. We describe our information practices in a detailed privacy policy that is posted on each of our consumer-facing websites and is attached as Exhibit A.

Policymakers have separately studied the privacy practices of major online publishers in a variety of settings, including Congressional hearings and recent proceedings conducted by the Federal Trade Commission and the Department of Commerce. We do not understand those practices to be the subject of your current inquiry.

Instead, your July 25th letter seeks information about practices described as “data brokerage” – *i.e.*, the sale of consumer personal information to third parties. Meredith does not sell consumer data to third parties but does operate a commercial list rental and data licensing business through a division of Meredith’s National Media Group known as Meredith Database Marketing Services (“DBMS”). DBMS is a very small enterprise both in relation to Meredith’s other operating units and in comparison to the other data companies that received your letter. To put DBMS’ operations in perspective, it accounts for significantly less than one percent of Meredith’s overall revenue and only four employees are dedicated to this business.

DBMS also differs from most, if not all, of the other companies involved in this inquiry in that the vast majority of the consumer records in its database relate to current or former Meredith customers. DBMS collects information only about consumers who have interacted directly with Meredith’s brands, with only one minor exception relating to the collection of crop, acreage and similar information about the operators of commercial farms and agriculture businesses.

Significantly, the FTC, in its final report on “Protecting Consumer Privacy in an Era of Rapid Change” (the “FTC Report”) refers to “data brokers” and “information brokers” as “non-consumer facing entit[ies].”¹ Similarly, each of the federal data broker bills referenced in the FTC Report – including legislation sponsored by members of the Bipartisan Privacy Caucus – defines an “information broker” as “a commercial entity whose business it is to collect, assemble, or maintain personal information concerning individuals *who are not current or former customers of such entity* in order to sell such information or provide access to such information to a non-affiliated third party in exchange for consideration.”² Under this definition, Meredith would not qualify as a “data broker” or “information broker” with respect to the vast majority of its list rental or data licensing operations.

¹ Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers,” March 2012, see pp. 17, 69, B-2, B-3.

² See Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act (DATA) of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011) (emphasis added).

Your July 25th letter emphasizes that consumers “often have little or no knowledge about the identity of data brokers, how they collect information and to which outside parties they sell or otherwise provide this information.” Unlike consumers whose data is collected by typical data brokers, the consumer subjects of Meredith’s information collection activities interact directly with Meredith and are therefore better able to learn about our practices and exercise related opt-out choices.

The core business for DBMS is the rental of lists of names and postal addresses of Meredith’s magazine subscribers and other customers to reputable third-party marketers for direct mail advertising purposes. These decades-old practices are described in both our online and offline privacy policies, which also include clear instructions about how consumers can opt out of the rental of their information to third-party marketers. Similar opt-out instructions are also printed on the masthead page of every issue of Meredith’s subscription magazines.³

As further described below, DBMS also offers list enhancement and data-append products, several of which DBMS simply resells for other data companies. These products are a very small part of the DBMS business. When DBMS acts as reseller, it does not collect, store or manage the licensed information. Other DBMS products do leverage information in Meredith’s consumer database to match consumers’ interests with marketers’ products and services. The information contained in that database includes information collected directly from Meredith customers when they interact with our company, as well as information that Meredith licenses from third-party data companies.

Meredith uses demographic, shopping behavior and other information licensed from third-party sources to better understand the audience that we and our advertising clients seek to engage and to sort our database into proprietary life stage clusters (such as “new parents,” “emerging families,” “new movers,” “empty nesters”) and interest-based “passion points” (such as “outdoors,” “pets,” “decorating,” “cooking,” “crafts,” “health and fitness”). We use these clusters to identify groups of consumers who are most likely to be interested in particular types of product offerings.

Our list rental and data licensing products are designed to help companies find those consumers who are most likely to be interested in their products and services, thereby avoiding inefficiency and increasing the likelihood that the offers consumers receive are actually responsive to consumers’ interests and needs. Meredith does not offer data products for determining eligibility for credit, insurance or employment. DBMS licenses its products for approved marketing purposes, which are stated in our license agreements. We verify compliance with these license restrictions, both through pre-campaign review and post-campaign monitoring facilitated by test addresses that we seed into our rented lists.

Your letter indicates a strong interest in commercial data practices involving children and teens. Meredith shares your concern for the privacy interests of America’s youngest consumers. DBMS does not offer lists or data products designed for target marketing to children or teens. Nor do we knowingly collect personal information from children or teens or create individual DBMS name and address profiles for consumers who are not adults. Consistent with Meredith’s focus on the family, home and parenting markets, we do obtain information from third-party data

³ See example attached as Exhibit B.

companies about the presence of children in households and the ages of those children. Parents may also voluntarily provide additional information about their children, including their gender and birthdays/due dates, when they register for our parenting websites. However, DBMS uses and licenses this information only in relation to individual records it maintains about adult members of a household, and the children's parents would be subjects of any related analysis and the intended recipients of any campaigns executed using the licensed data.

In sum, the scale and nature of our list rental and data licensing business differentiate Meredith from the business models that appear to be the focus of your "data brokerage" inquiry. We recognize, however, that every company that stores information about consumers must safeguard and manage that data responsibly. We believe we are meeting those obligations. In Meredith's case, the affected consumers are also our customers. We have powerful incentives to preserve their trust.

Meredith appreciates and shares your interest in the important topic of commercial data practices. To help you and other members of Congress assess the benefits and burdens of further regulation in this area, we have enclosed detailed responses to the specific questions posed in your recent letter. For our part, we believe that industry self-regulation is the most efficient and effective means of ensuring that sound privacy practices evolve in an era of fast-changing technology and new business models. In areas such as online behavioral advertising, a broad coalition of industry stakeholders has demonstrated that self-regulation delivers robust yet flexible standards that adapt quickly to technological changes and are enforceable against participating companies. Industry leaders have already convened to discuss a self-regulatory response to the proposals on "data brokers" put forward earlier this year by the Federal Trade Commission. We believe that lawmakers should give these efforts an opportunity to succeed before intervening with new legislation.

Sincerely,



Stephen M. Lacy
Chairman and CEO



RESPONSE TO INFORMATION REQUESTS

Data Sources (Question 1)

The majority of consumer data used in our DBMS business is provided by consumers themselves directly to Meredith as we provide subscriptions, digital content or other products and services under our brands.

Nine companies and government agencies have provided additional consumer data to Meredith that has been used by our DBMS business since January 2009. These sources include Axciom Corp., InfoGroup, Inc., Kantar Retail, Nielsen Claritas and the United States Department of Agriculture Farm Service Agency. Our contracts with the four other information suppliers prevent us from publishing their names. Although DBMS has used some of the information supplied by these companies in its list rental and data licensing products, as stated in our cover letter, Meredith primarily uses this information it collects about consumers to better understand the audience that we and our advertising clients seek to engage.

Meredith's online privacy policy expressly discloses that information collected from our customers may be combined with contact, demographic and other information obtained from third-party commercial data suppliers and public database sources:

"We may combine the information we collect through the Services with other information that we obtain about you, your computer, and/or device from other companies and sources, including third-party data suppliers and public databases. The following are examples of information we may collect from other sources:

- *Name, postal address, email address and telephone number;*
- *Demographic data, such as age, gender, and income level;*
- *Your interests and purchase behavior*

Types of Data Used in DBMS (Question 2)

All of the consumer information we collect in connection with our DBMS products is related to current or former Meredith customers with the exception of records for certain farmers and growers included in our small but historically important agricultural database⁴. The categories of information we collect for use in our DBMS products are summarized below:

Demographics

- Adult Age
- Presence and Age of Children
- Marital Status

⁴ In our agricultural database, we supplement information we collect about subscribers to our *Successful Farming* magazine and related website with information about other members of the farming community. For years, we obtained this supplemental information from the United States Department of Agriculture's Farm Service Agency. This data is currently supplied by a commercial data provider. Clients use lists compiled from our agricultural database predominantly for business-to-business marketing as opposed to consumer marketing purposes.

- Ethnicity
- Household Income
- Household Net Worth
- Home Value
- Household Size
- Home Ownership by Dwelling Unit
- Occupation
- Credit Card Membership
- Life Stages⁵

Shopping Information

- Purchases By Category
- Computers and Internet Access
- Product Ownership/Intent to Purchase
- Financial Products (owned or plan to buy)
- Store Shopping Preference
- Retail Shopping Data

Lifestyle and Passions

- Passion Points⁶
- Collectors
- Music
- Reading
- Sports
- Travel
- Hobbies
- Charitable Cause Donors

Nutrition and Health Interests

- Nutrition and Diet Interests
- Health Interests

Agriculture

- Owner/Operator
- Absentee Owner
- Farm Size
- Irrigated Acreage
- Crop Acreage (by crop type)
- Herd Size (by livestock type)
- Horses owned
- Tractor Type

⁵ “Life Stages” are proprietary cluster categories created by Meredith such as “new parents,” “new home owners” and “empty nesters.”

⁶ “Passion Points” reflect primary areas of interest that DBMS attributes to subgroups of customers, such as “cooking,” “gardening,” and “decorating.”

- Truck Type
- ATV Type
- Seed/Chemical Brand Preferences

Methods of Data Collection (Question 3)

Meredith's consumer data is collected both internally when customers interact with our publications and digital properties and to a much lesser degree externally from third-party data suppliers. The data we gather directly from our customers falls into two categories: (1) information that customers voluntarily supply when they subscribe to our periodicals, register for our websites, applications or other services, initiate transactions, participate in surveys or otherwise communicate directly with Meredith; and (2) the information collected when customers use Meredith's websites and other interactive services. Only the first category of internally-collected consumer data has been used in our DBMS products.

Much of the information we use to build our DBMS products is sourced from magazine subscriptions and website registration transactions. Magazine subscription forms typically elicit name, postal and email address information. Customers may register on Meredith's various websites to create accounts through which they can manage the Meredith services they receive. Information typically collected during these registrations includes name, postal address, email address and communications preferences, such as which newsletters the customer would like to receive. Additionally, Meredith may inquire as to the consumer's age, gender, hobbies and interests. All of this registration information may be used by DBMS.

Social Media and Mobile Platforms. No data collected from social media sources is used in the DBMS business except for the limited name, address and email address information collected from consumers when they register for newsletters or the occasional promotional sweepstakes using forms available on Meredith social media sites.

Similarly, DBMS does not currently use information derived from customers' mobile use of our services in any of its products except for name, postal and email address information that is voluntarily supplied by the user and the fact that a consumer is a mobile device user.

DBMS Data Products and Services (Question 4)

DBMS products that use information collected from and about consumers consist mostly of list rental products. A much smaller segment of DBMS business is composed of data installation products (also known as "list enhancements" or "data licensing"), customer profiling, predictive modeling, and custom data collection services.

DBMS rents name and postal lists and licenses other data about consumers to reputable companies for the purpose of marketing consumer products and services directly to consumers.

DBMS clients include companies in the catalog/merchandise, services, retail, agriculture, auto, pharmaceutical and food industries. Meredith also rents lists and licenses data to nonprofit organizations to help them direct membership, awareness and charitable fundraising campaigns. Political campaigns and organizations also rent lists from DBMS and we have recently worked with major organizations and campaign committees for both national political parties.

DBMS does not rent lists or license data for purposes of making firm offers of credit or insurance or determinations of consumers' eligibility for credit, insurance or employment. To our knowledge, no DBMS client has used Meredith data for these purposes. Accordingly, DBMS is not a "consumer reporting agency" as defined in the Fair Credit Reporting Act. Additionally, DBMS products do not involve "lead generation," as that term is commonly used in the marketing industry.

List Rental Products. DBMS' core list rental products generally consist of names and postal address records selected from Meredith's customer database based on data parameters requested by the client. The list of names and postal addresses is provided to the client so that it may execute one or more direct mail campaigns for products or services specified in a list rental agreement. DBMS also offers email list rental products but in these programs, DBMS does not actually provide a list of consumer email addresses to the client. Instead, DBMS manages deployments of email marketing campaigns on the client's behalf. The campaign uses Meredith data for purposes of developing the distribution list and uses opt-in email addresses matched to records on the distribution list by a third-party deployment company.

Data Installation Products. DBMS also offers licensed data installation products, typically referred to as "list enhancements," in which DBMS provides to a client certain segments of data that the client can then "overlay" on its own database. As explained below, only a small subset of the information in Meredith's consumer database is made available for list enhancement purposes.

Customer Profile Analysis. DBMS also offers customer profiling services to our clients. In these programs, the client furnishes a sample of its customers to DBMS that we match to profiles in Meredith's database and analyze with respect to criteria that are relevant to the client's desired market. The product of this analysis is a set of reports that profile the population represented by the client sample against relevant data segments. These reports take the form of aggregated statistics rather than individually identifiable data.

Predictive Modeling. When a client orders predictive modeling services, DBMS matches a sample of the client's current high-value customers (for example, repeat buyers) to consumer records in DBMS' database, identifying which characteristics distinguish those consumers. DBMS then generates a list of prospective customers – names and postal addresses – that possess characteristics similar to the client's sample group. The goal of this process is to identify the characteristics that differentiate client customers with known, desirable purchasing histories and then replicate those characteristics in a prospect list drawn from Meredith's consumer database.

Custom Data Collection. In these programs, DBMS designs and fields custom market research surveys for clients that collect information directly from consumers. Custom data collection is also a very small segment of DBMS's business and has been used primarily by companies in the agriculture sector for business-to-business marketing purposes.

File Append Services. DBMS offers certain email and mobile telephone number "append" and "reverse append" products as a reseller for a third-party data company. In the email append programs, the client provides to the third-party vendor a file of names and postal addresses, which is matched to records in the vendor's database of opt-in email addresses. The

vendor then sends emails to the matched customers requesting permission for the client to begin sending them email offers. These email solicitations present both opt-in and opt-out choices to the consumer. A confirmed opt-in email list is then returned to the client by the vendor for use in the client's email marketing programs.

Clients that order email reverse-append services provide a list of email addresses to which the vendor will attach postal addresses drawn from matched records in its database. The mobile phone number append products are structured in the same way as the email products described above. To date, DBMS has not sold any of these latter programs to its clients.

Meredith's consumer database is not used to create these email or mobile phone number append services; all of the information appended to the client's files is supplied directly by the third-party vendor. Meredith does not store, manage or transfer any of the licensed email or mobile phone number data involved in these programs.

Data Sources for DBMS Products. DBMS may use information from any of the data categories summarized in response to question 2, above, in its internal analytics to select name and postal address lists for a particular client and to perform customer profile analysis and predictive modeling.

The information available for licensing through DBMS' list enhancement products, however, is much more limited. DBMS only licenses the following types of information to clients: "Life Stages" and "Passion Points"; "Intender data" (*i.e.*, the consumer's intention to landscape, remodel, decorate, or move); Meredith product subscription history (*i.e.*, order date, last activity date, expiration date, subscription source); New Parent data (*i.e.*, birthdates/due dates of children, first-time parent or multi-birth indicator); summarized shopping data (*i.e.*, recency of purchases, frequency of purchases, spending levels); and agriculture data (farm interest, size of farm in acres, crops by acre, livestock by type, tractor and truck brands, seed and chemical brand preferences).

Restrictions on Use of Rented/Licensed Consumer Data. DBMS enters into an agreement with each of its clients that typically limits the purposes for which the rented list or licensed data may be used to a specifically identified marketing campaign or program. Our agreements contain other restrictions: for example, consumer information provided by Meredith may not be used for telephone or face-to-face solicitation and our contracts typically impose certain data security requirements on our clients. Additionally, the agreements we use for our list rental products generally provide that Meredith must review and approve any client marketing materials that will be mailed using the rented postal list prior to their distribution. To ensure that clients do not exceed the parameters of our license agreement, DBMS also "seeds" rented lists with test addresses that are used to track clients' use of our data.

Access, Correction, Deletion and Opt-Out (Questions 5 – 9)

Meredith offers a variety of mechanisms through which our customers can access, correct, and make choices about information that we maintain and use.

Access and Correction. Our customers may access and edit personally identifiable information they provide to us when they subscribe to one of our periodicals or register for one

of our websites. They do so by using an electronic form accessible from the customer service tab on any of our websites. Instructions about how to use these features are clearly posted on our websites.

The masthead of each Meredith magazine also directs customers to log on to the publication's website to change their addresses and inquire about their subscriptions. If a customer does not wish to use an online account, he or she may contact the publication by telephone or by postal mail. Relevant telephone numbers and postal addresses for such inquiries are provided in each issue. Information that can be edited through these means includes customer name, postal addresses, email address, email and Meredith product preferences, and any information that the consumer has stored in a community profile.

We restrict customers' access beyond the foregoing categories of data. This policy is consistent with accepted commercial practices and the FTC Report, which notes the impracticality of providing access to data that is being used for marketing purposes. The FTC Report specifically states that "companies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain."⁷ The FTC notes that the only "harm" consumers might experience from inaccurate marketing data is an "irrelevant advertisement." The FTC further noted that heightened access and accuracy standards for marketing data would actually require the addition of more personally identifiable information to marketing databases in order to permit authentication of individuals who request access or changes to these records.⁸

Opt-Out and Deletion. Meredith offers several opt-out options to customers, allowing them to suppress our use of their data for purposes of third-party offers and/or Meredith offers. By completing a form provided in our offline privacy policy, customers may exclude their names and postal addresses from any lists or list enhancement files that we provide to DBMS clients. Customers simply check an appropriate box to opt-out, then provide their names and postal addresses so that we can identify who is making the request.

Additionally, a notice in the masthead of each Meredith publication explains that the publication's subscriber list may be shared with third parties whose products Meredith believes may be of interest to its customers. The same notice provides instructions about how customers can prevent the sharing of their information by sending a request together with magazine mailing label to a designated Meredith postal address. Before providing lists or licensed data products to a client, DBMS also suppresses the names and addresses of any consumers that appear on the Direct Marketing Association suppression list.

When a customer opts out of allowing his or her information to be used as part of a DBMS product, the customer's information is retained in our database but is flagged as suppressed for list rental and data licensing purposes. Similarly, when a customer opts out of receiving promotions directly from Meredith, his or her customer information is retained but suppressed for purposes of our internal marketing efforts. To ensure that a customer's opt-out request is honored, it is necessary to maintain a record of the customer's choice. If we deleted a customer's record after receiving an opt-out request, we would have no way of honoring the

⁷ FTC Report at p. 30.

⁸ See FTC Report at p. 29.

customer's preferences if he or she reappeared in our database as a result of a subsequent magazine subscription order or other transaction with one of our properties.

According to our records, since January 2009, Meredith has logged more than six million opt-out requests for our DBMS business. Our policy is to honor every request we receive.

Data Storage and Security (Questions 10 – 11)

Meredith stores the consumer data used by our DBMS division in a database format using industry-standard database technology. This consumer database is protected within Meredith's corporate IT security framework, which was developed using risk management principles and guidelines derived from the ISO-27002 code of practice for information security, Sarbanes-Oxley general controls and Payment Card Industry Data Security Standards (PCI DSS).

A Meredith IT Security, Compliance and Continuity team develops, implements and maintains our Information Security Policy, which is designed to protect the consumer data used by DBMS and Meredith's other information resources against unauthorized access, disclosure, modification, transfer, storage, misuse and destruction. A copy of Meredith's Information Security Policy is attached as Exhibit C.

Meredith's uses industry-standard encryption protocols when transferring data from DBMS to outside entities. These encryption protocols include secure sockets layer (SSL), transport layer security (TLS) and Pretty Good Privacy (PGP).

Review Process for DBMS Clients (Question 12)

DBMS performs due diligence reviews of prospective list rental clients and data licensees to ensure that they are legitimate and reputable companies or organizations. Such due diligence efforts typically involve a review of the Better Business Bureau's databases and Dunn & Bradstreet data, as well as other publicly-available information about the prospective client. DBMS has declined to take business from many prospective clients as a result of this review.

Once Meredith and its client have executed the relevant agreements, which typically restrict the use of DBMS data to specific marketing purposes (*e.g.*, the use of rented lists to direct mail offers for particular client products or product lines), DBMS employs other checks, such as pre-distribution review of client mailings, and post-contract monitoring of client communications sent to pre-seeded test addresses, to ensure that the client's use of Meredith's customer data conforms to the licensed purposes.

Customer Notice (Question 13)

Our information practices are detailed in our online and offline privacy policies attached as Exhibit A. As noted above, we also publish a notice regarding our list rental practices and related opt-out choices on the masthead pages of our magazines.

Children and Teens (Question 14)

As noted above, with the limited exception of certain information obtained about the operators of agricultural businesses (all of whom obviously would be adults), DBMS only collects and licenses personal information about current and former Meredith customers. Meredith acquires its customer relationships through consumers' engagement with our portfolio of publications and digital properties that are designed to appeal to an audience of adult consumers – predominantly women age 25 and older. None of our media properties is geared to the interests of children or teens.

As stated in our online privacy policy, Meredith does not knowingly collect information online from children under the age of 13 and we expressly discourage children from trying to register for any of Meredith's services or providing any personally identifying information.

DBMS does not design list rental or data products for purposes of reaching consumers who are not adults and DBMS does not create individual name and address profiles for children or teenagers.

Consistent with Meredith's focus on the family, home and parenting markets, some of the demographic data that DBMS obtains from third-party data companies includes information about the presence of children in households and their respective ages. Parents may also voluntarily supply additional information about their children, including their gender, birthdays/due dates, when they register for our parenting websites. However, DBMS analyzes and licenses this information only in relation to the records it maintains about adult members of the household, and the adult parents would be the intended recipients of any campaigns using the licensed data.

Attached:

- Exhibit A – Privacy Policies (online and offline)
- Exhibit B – Sample Masthead
- Exhibit C – Information Security Policy

Meredith Online Privacy Policy

Effective Date: April 5, 2012

Online Privacy Policy	Your California Privacy Rights
Offline Privacy Policy	
Visitor Agreement	

Online Privacy Policy

Welcome! This Online Privacy Policy applies to your use of websites, interactive services and mobile device applications provided by Meredith Corporation or our affiliates (collectively, "Meredith," "we" or "us") and that display an authorized link to this policy (collectively, the "Services"). This Online Privacy Policy applies only to the information we collect online through the Services. Please click [here](#) to see our separate Offline Privacy Policy.

By using any of our Services, you agree that this Online Privacy Policy and our [Visitor Agreement](#) govern your use of our Services and any dispute concerning the Services. Please take a few minutes to read them before using or registering to access our Services.

This Policy describes our privacy practices regarding:

Children under 13	Sites to Which We Link
Information Collected Through Our Services	How to Correct or Update Your Information
Information We May Obtain from Other Sources	Security, Retention and Storage of Information
How We Use the Information We Collect	Changes to Our Online Privacy Policy
How We Disclose Information and Your Related Opt-Out Choices	

If you have questions about this Online Privacy Policy, please contact us at privacy@meredith.com

[Return to top](#)

Children Under 13:

Meredith cares about protecting the privacy of children. We won't knowingly allow anyone under the age of 13 to provide us any personally identifying information online. Children should always get permission from their parents before sending any personal information about themselves (such as their names, email addresses, and phone numbers) over the Internet, to us or to anyone else. We encourage you to become involved in your children's online experience, and to share your knowledge and experience with your young ones. If you're under 13, please do not register for any of our Services or provide us with any personally identifying information (such as your name, email address or phone number).

[Return to top](#)

Information Collected Through Our Services:

The information we gather through our Services falls into two categories: (1) information you voluntarily supply to us when you register, initiate transactions or communicate with us through the Services, and (2) information collected automatically as you use our Services. Third-party providers and advertisers featured on, or linked to from, our Services may also gather information through processes that we don't control and subject to their own separate privacy policies, which may differ from ours.

Registration and Other Personally Identifying Information. You may register to use certain features of our Services. When you register, we may collect personally identifying information, including your name, postal address, email address, user name and password, reminder questions and answers and communications preferences, such as which newsletters you would like to receive. We may also ask for information about age, gender, hobbies, interests and the like, but you're free to register for most of our Services without providing this additional information. When you register for one of our Services, the information you provide may be added to a centralized Meredith database so that you may be simultaneously registered for our other Services as well. In addition, when you use various aspects of our Services, we may ask you for personally identifying information, including when you order products, complete a survey, enter a contest, or report a problem with our Services. We and our authorized third-party service providers use this information to process orders, tailor our Services to your interests or otherwise improve our Services. We may also collect contact information for other individuals when you use the sharing tools available within some of our Services to forward content or offers to your friends and associates. We use this information to facilitate the communications that you request. Please note that if you use any "send-to-a-friend" features of our Services, your email address may be included in the communication sent to your friend.

Contests and Other Promotions. From time to time, we may offer contests, sweepstakes or other promotions. Participation in these promotions may require registration for our Services (see Registration and Other Personally Identifying Information, above). If you participate in these promotions, we collect contact information such as your name, address, and email address and we may share this information with co-sponsors or other third parties involved in the presentation of the promotion that we identify in the rules or entry materials. We don't control these third parties' privacy practices, and our Privacy Policy does not apply to their collection and use of your information. We may also share some of your entry information with third parties or the public in connection with the administration of the promotion, such as winner selection and prize fulfillment, and as permitted by the promotion's official rules, such as on a winners' list.

Information Collected Automatically When You Use Our Services. Meredith or third-party contractors acting on our behalf may collect certain information automatically when you use our Services, including:

- Your browser type, language, plug-ins, Internet domain and operating system;
- Your Internet Protocol (IP) address (a numerical address assigned to your computer by your Internet service provider so that other computers connected to the Internet can communicate with you online) that can sometimes be used to derive your general geographic area;
- The site you visited before visiting a Meredith website and the site you visited after visiting a Meredith website;
- Web pages and advertisements you view and links you click on while navigating within our Services;
- Unique identifiers, including mobile device identification numbers, that can identify the physical location of such devices in accordance with applicable law;
- Information collected through cookies, web beacons and other tracking technologies (see additional descriptions of these terms below);
- Information about your interactions with our video content, such as the type of content viewed on our Services; information about your interactions with our email messages, such as the links you click on and whether you open or forward a message; and standard server log information.

Personalization and Tracking Technologies. Like most website and mobile application operators, we, or third parties acting on our behalf, use embedded scripts, "cookies," web beacons and other similar technologies to operate our Services.

Cookies are small amounts of data (often containing a unique identifier) that are stored in separate files within your computer's Internet browser. Cookies are accessed and recorded by the websites you visit, and by the companies that deliver the advertisements you see on websites, so they can recognize the same browser navigating online.

We use cookies for the following general purposes:

- To help us recognize your browser as a previous visitor and save and remember any preferences that may have been set while your browser was visiting one of our websites. For example, if you register for a Meredith Service, we may save your username and password, so you do not have to re-enter them each time you visit.
- To help control the display of advertisements and customize the content and advertisements you see while using our Services and sometimes while visiting other websites online.
- To help us measure and analyze visitor traffic and usage patterns and to improve the quality and effectiveness of our content, features, advertisements, and other communications.

Third-party companies that provide some of the tools and features accessible through our Services and advertisers and other companies involved in the delivery of the advertisements that you see while using our Services and other websites also may place cookies within your browser. We do not have access to these cookies and do not control how they may be used. You can set your browser to accept or reject most cookies, or to notify you when a cookie is set. (Each browser is different, so check the "Help" menu of your browser to learn how to change your cookie preferences.) It is up to you whether to allow us or third parties to send you or to set cookies, but if you block cookies, you may not be able to view or access some of the features of our Services. Please be aware that certain browsers cannot block or delete so-called "Flash" cookies, which use a feature of the Adobe Flash video player to store information on your computer. For information about how to delete Flash cookies, please visit the Adobe website [here](#).

Web Beacons and Other Tracking Technologies. We and our service providers and other third-party companies involved in the delivery of advertisements you see on our Services and/or while visiting other unaffiliated websites may also use scripts, web beacons and/or similar technologies, to collect information about your use of our Services. Web beacons (sometimes called "transparent GIFs," "clear GIFs," or "pixel tags") embed a small graphic image (usually invisible) on a web page or in an email. When your browser downloads a web beacon, the server that sends the corresponding image to your browser can recognize and store certain types of information such as cookies previously set, the time and date that you viewed the page embedded with the beacon and a description of that page. We use web beacons to improve your experience using our Services, including to provide you with content, advertising and offers customized to your interests, and to understand whether our users read email messages and click on links contained within those messages.

Mobile Device IDs and Location-Based Information. Certain mobile devices, including smart phones and tablet devices, contain unique device IDs that can be used to identify their physical location. Mobile devices also typically transmit caller ID data (which may include a phone number) when used to transmit a telephone call or text message. When you use mobile devices to access our Services, we may collect and transmit unique device IDs and collect caller ID data, information about your wireless carrier, the make, model and operating system of your device and information about how you navigate within our Service. With your consent, we also may use precise geolocation technology such as GPS or WiFi triangulation to collect information about the exact location of your mobile device. We use this information to provide you the content and services you request, tell you about offers we think you will value, and improve your experience using our mobile applications and other Services.

Information Collected in Connection With Ad Serving, Targeting and Analytics. We and our service providers may use information collected when you use our Services to serve interest-based advertisements on our Services and on other third-party websites that participate in advertising networks that we operate. The data collection for our networks currently is managed by our service provider, Collective. Meredith follows the Self Regulatory Principles for Online Behavioral advertising released by the Digital Advertising Alliance ("DAA") in July 2009. To learn more about the Principles

and to opt-out of the cookies used to tailor interest-based advertising on the third-party sites in our networks, visit <http://www.aboutads.info/>. You can also easily opt-out of these targeted ads by clicking on the AdChoices icon located in the footer of our web sites.

We also may work with other third-party advertising companies and data providers to target and serve some of the advertisements you see on our Services and on other websites, to send emails on our behalf, and to provide related analytics, forecasting, optimization and audience segmentation services. These companies may use their own cookies, web beacons and similar technologies to collect navigation information from our users that they may use, sometimes in conjunction with similar information gathered through other websites, to deliver advertisements tailored to match perceived user interests and/or for other purposes. To enable you to receive customized ads, content or services, some of these companies may also place or recognize a unique cookie on your browser that reflects de-identified demographic data or other information about you that they obtained from third-party data suppliers. To enable these cookies, we may share with these companies your email address or other registration information in an encrypted format (i.e. hashed non-human readable form) solely for the purpose of matching you to a relevant demographic profile. No personally identifying data will be captured or used in the cookies. To opt out of these cookies, please click on the AdChoices icon located in the footer of our web sites or you can go to <http://www.aboutads.info/>

Most of the third-party advertising and data companies we work with, including DoubleClick and Google, are members of the Network Advertising Initiative (“NAI”) and/or the DAA). To learn more about the information collection practices of NAI and DAA members and your ability to opt-out of their information collection activities, please visit the NAI’s website [here](#), or the DAA’s website (and opt-out mechanism) at <http://www.aboutads.info/>. We also engage Omniture, a third party, to track and analyze usage and browsing patterns of our users. For information about Omniture’s information collection practices and related opt-out choices, click [here](#). Many of our advertisers also engage other third-party vendors to help them deliver advertisements tailored to your interests, and evaluate and improve the effectiveness of their advertising campaigns. We do not have access to the information these third parties may collect and this Policy does not cover their information practices. You can opt out of the use of cookies by many of these third-party vendors to tailor advertising to you by visiting <http://www.aboutads.info/>.

Social Network Posting Tools and “Share” Features. You can access various social network posting and sharing tools through our Services that are operated by third parties, including a “share” button that allows you to post links to content and features that you believe will be of interest to others on your social network pages. When you use one of these sharing tools, the third-party company that operates the tool may be collecting information about your browser, device and online activity through its own tracking technologies and subject to its own separate privacy policy, which may differ from ours. The “Share” button functionality available within many of our Services is provided by Gigya, Inc. and its privacy policy is available [here](#).

Nielsen Online Campaign Ratings Service. Some of our advertisers may participate in a program operated by the Nielsen Company to develop an Online Campaign Ratings service that is comparable to Nielsen’s television ratings. When one of their ads appears on our Services, it may contain a web beacon that will record your exposure to the ad, read certain cookies on your browser, and forward this information to one or more operators of third-party websites or other online service on which you may have registered. If the third-party operator recognizes a cookie that identifies you as one of its registered users, it will append the impression data it receives, which may identify you as a user our Services, with age and gender information before returning the data to Nielsen. Nielsen aggregates the data it receives about a given campaign to create ratings reports for advertisers and publishers. According to Nielsen, these reports measure campaign performance on an aggregate level within various demographic categories and do not identify you personally. For more information about Nielsen’s information collection practices and any related opt-out choices that Nielsen offers, please see the Nielsen.com privacy policy [here](#).

[Return to top](#)

Information We May Obtain From Other Sources:

We may combine the information we collect through the Services with other information that we obtain about you, your computer, and/or device from other companies and sources, including third-party data suppliers and public databases. The following are examples of information we may collect from other sources:

- Name, postal address, email address and telephone number;
- Demographic data, such as age, gender, and income level;
- Your interests and purchase behavior;
- Publicly-visible data, such as your posts and submissions to blogs, video-sharing services, and other interactive forums; and
- Other navigation data, such as web sites visited and advertisements viewed or clicked on.

[Return to top](#)

How We Use The Information We Collect:

Our primary goal in collecting information is to provide you with a customized experience when using our Services and to make them more valuable to you. Because our Services are supported by advertising, we also use the information we collect to help advertisers efficiently reach consumers who are most likely to be interested in their products and services. We only use payment and identity verification information, such as credit card numbers, driver's license numbers, social security numbers, or comparable national identifiers as necessary to complete a particular transaction, provide a requested service, enforce legal rights or comply with applicable law.

In addition, we and our authorized service providers generally use other information that we collect about you to:

- Analyze, operate and improve our Services, and fulfill your requests for products, services, and information, including to send you electronic newsletters;
- Enable you to participate in features such as surveys, polls, sweepstakes, and message boards;
- Provide you with special offers and promotions from companies within our corporate family, and select third parties in accordance with applicable law;
- Customize the content you see when you use our Services;
- Develop and provide advertising tailored to your interests, including advertising that you see on our Services and on third-party websites;
- Prevent potentially prohibited or illegal activities and enforce our Visitor Agreement;
- Conduct market analysis, traffic flow analysis and related reporting; and
- For any other purposes disclosed to you at the time we collect your information or pursuant to your consent.

[Return to top](#)

How We Disclose Information and Your Related Opt-out Choices:

Except as otherwise expressly noted herein or within the Services, we may share any information that we collect through our Services, including without limitation, your name, postal address (and any other information we combine with that information) with our Meredith-affiliated companies, our provider partners and service providers, and with carefully selected third-party marketers of products and services potentially of interest to you. To remove your name and postal address from lists that we sell or rent to third parties for their direct marketing purposes, please use the postal list opt-out form available here "opt-out" form or send your request to us in a letter addressed to Meredith Corporation, Opt-Out Postal, Attn: Circulation, 1716 Locust Street, Des Moines, Iowa 50309). Without your consent, we will not sell or rent your email address to unaffiliated third parties for their email marketing purposes. If you use our Services to sign up for special email offers from third-party advertisers, we will share your email address and any other information you provided with your request with the advertisers

you selected. If you decide you no longer want to receive these emails, simply follow the advertiser's unsubscribe link or instructions that should be included in every commercial message you receive. If you choose to subscribe to any of Meredith's newsletters or commercial email lists, you can unsubscribe at any time by following the unsubscribe link at the bottom of each message or by visiting our Email Preferences page on our sites and updating your preferences.

Provider Partners and Service Providers. To make your experience with our Services more useful and enjoyable, we may offer some features (such as chat rooms and email newsletters) in conjunction with third-party providers ("Provider Partners") that specialize in operating such services. We share with each of these Provider Partners such information as is useful or necessary to provide you with the services we offer through that Provider Partner. We also contract with other companies to provide specialized services to us, including credit-card and billing processing, shipping, marketing, email and text message distribution, data processing, website analytics and promotions management. We reserve the right to share with these companies any information we collect about you provided that they commit not to use the information for purposes other than to perform the services we request.

Aggregated Information. We may combine information that we collect about you with information that we collect about other users of our Services and share it in a form that does not identify you personally. We may use aggregated information or other anonymous information and disclose it to third parties as we see fit.

Information You Post to Blogs, Discussion Forums and Community or Social Networking Areas. Keep in mind that any information that you choose to post to blogs, discussion forums, or other community or social networking services that we offer can be seen, collected and used by anyone who has access to the applicable service. We cannot be responsible for any unauthorized third-party use of such information.

Legal Compliance, Business Transfers and Other Disclosures. Notwithstanding anything to the contrary stated herein or within our Services, we may occasionally release information about users of our Services when we deem such release appropriate to comply with law, respond to compulsory process or law enforcement requests, enforce our [Visitor Agreement](#), or protect the rights, property or safety of users of our Services, the public, Meredith Corporation, our affiliates, or any third party. Over time, we may reorganize or transfer various assets and lines of business. Notwithstanding anything to the contrary stated herein or on our Services, we reserve the right to disclose or transfer any information we collect to third parties in connection with any proposed or actual purchase, sale, lease, merger, foreclosure, liquidation, amalgamation or any other type of acquisition, disposal, transfer, conveyance or financing of all or any portion of Meredith or our affiliates.

[Return to top](#)

Sites to Which We Link:

We also may provide links to other websites or services, and provide access to products and services offered by third parties, whose privacy policies we don't control.

[Return to top](#)

How to Correct or Update Your Information:

Meredith Corporation believes in providing you with the ability to access and edit the personally identifying information that you have provided to us through our Services. To update this information, please visit the "My Account" area or comparable feature of the Service you used to enter your information. If you cannot locate such a feature, send us an email at privacy@meredith.com.

[Return to top](#)

Security, Retention and Storage of Information:

We use commercially reasonable procedures to protect the personally-identifying information that we collect. No security system is impenetrable, however. We cannot guarantee the security of our databases, nor can we guarantee that information you supply won't be intercepted while being transmitted to us over the Internet. Please see our [Visitor Agreement](#) for more information related to posting materials on our Services including our use of such materials.

For the purposes set out in this Online Privacy Policy, personally-identifying information may be transferred to, processed, stored and accessed by us, our affiliates and our unaffiliated service providers in the United States and in other jurisdictions where we or they operate. Courts and other authorities in these jurisdictions may, in certain circumstances, be entitled to access your personally-identifying information. By using the Services, you consent to this transfer, processing, storage and access of your personally-identifying information in and/or outside of the jurisdiction in which you reside.

[Return to top](#)

Changes to Our Online Privacy Policy:

Digital technology is rapidly evolving. If we decide to change our Privacy Policy in the future, we'll post the changes here and indicate at the top of the policy the last date on which it was updated. Unless otherwise noted, all changes will be effective when posted.

[Return to top](#)

YOUR CALIFORNIA PRIVACY RIGHTS

(As provided by California Civil Code Section 1798.83)

California residents have the right to request and obtain from us, once a year and free of charge, a list of the third parties to whom we have disclosed certain types of personal information (if any) for their direct marketing purposes in the prior calendar year. At our option, we may respond to such requests by providing instructions about how our users can exercise their options to prevent our disclosure of personal information to third parties for their direct marketing purposes. You can read these instructions above in the section of our Online Privacy Policy titled *"How We Disclose Information and Your Related Opt-out Choices."* Or, if you are a California resident and prefer that we send you a separate description of these opt-out choices, please email your request to privacy@meredith.com

Better Homes and Gardens.

James T. Carr

President, Better Homes and Gardens

Anthony P. Imperato
Vice President, Publisher

Julie V. Baker
Vice President, Associate Publisher, Marketing

Cathy Dropkin
Eastern Advertising Director

Gary Wenstrup
Midwest Advertising Director

Advertising Sales

NEW YORK

Kristine Cronin, Janine Krause, Melissa Morales Langley,
Susan Schwartzman, Account Executives
Claire Franczyk, Danielle Zahavi, Assistants

CHICAGO

Emily Bâby, Tiffany Erickson, Maureen Powell,
Vickie Sandberg-McNay, Account Executives
Nicole Jacobson, Assistant

DETROIT

Karen Barnhart, Manager; Kim Kitchen, Assistant

LOS ANGELES

Isabella Carrado, Manager; Kristen Schoen, Assistant

SAN FRANCISCO

Janet Davy, Manager; Michelle Kwan, Assistant

DIRECT MEDIA

Grace Chung, Advertising Director
Jill O'Toole, Assistant

TRAVEL

Jodie Burlog Schafer, National Travel Director

Marketing

Denise Basini, Strategic Marketing Director; Kristen Stucchio Suarez, Integrated Marketing Director;
Christina Godlewski, Senior Integrated Marketing Manager; Gina Salvatini, Associate Integrated Marketing Manager;
Stefania Trampusch, Creative Director; Shana Hale, Associate Art Director; Karla Chrzanowski, Brand Development Director;
Melissa Aleevski, Sales Development Director; Rebecca Griffin, Sales/Marketing Coordinator

National Media Group Communications

Diana Terwilliger-Silberfein, Research Director; Kim Pasiri, Associate Research Director; Jon Macarthy, Consumer Marketing Director;
Ron Clingman, Business Director; Randi Neer, Advertising Business Manager; Jan Sims, Advertising Operations Director;
John Beard, Production Director; April Gross, Courtney Coles, Associate Advertising Operations Managers;
Pam Hutchcroft, Production Traffic Supervisor; Elise Contarsy, Bradford W. S. Hong, Brand Licensing;
Amanda Cortese, Associate Director, Brand and Business Communications; Christina Peletto, Senior Media Relations Manager
For help with your subscription or billing, call 800/374-4244.

Chief Development Officer: John S. Zieser Vice President of Development: David Johnson

Meredith National Media Group

President | TOM HARTY

EXECUTIVE VICE PRESIDENTS

President, Media Sales | RICHARD PORTER
President, Better Homes and Gardens | JAMES T. CARR
President, Parent's Network | CAREY WITMER
President, Women's Lifestyle | THOMAS WITSCHI
Creative Content Leader | GAYLE GOODSON BUTLER
Chief Marketing Officer | NANCY WEBER
Chief Digital Officer | LIZ SCHMEL
Chief Revenue Officer | MICHAEL BROWNSTEIN
Chief Innovation Officer | JEANNINE SHAO COLLINS
General Manager | MIKE RIGGS
Director Operations & Business Development | DOUG OLSON

SENIOR VICE PRESIDENTS

Meredith Women's Network | LAUREN WITENER
Chief Technology Officer | JACK GOLDBERG
Audience Development and Commerce | ANDY WALSON

VICE PRESIDENTS

Consumer Marketing | JANET DONNELLY
Corporate Marketing | STEPHANIE CONNOLLY
Direct Media | PATTI FOLLO
Research Solutions | BRITA WARE
Communications | PATRICK TAYLOR
Newsstand | MARK PETERSON



Chairman and Chief Executive Officer | Stephen M. Lacy

President, Meredith Local Media Group | Paul Karpowicz

Vice Chairman | Mell Meredith Frazier

In Memoriam | E. T. Meredith III, 1933-2003



Our subscribers list is occasionally made available to carefully selected firms whose products may be of interest to you. If you prefer not to receive information from these companies by mail or by phone, please let us know. Send your request along with your mailing label to Magazine Customer Service, P.O. Box 37503, Boone, IA 50037-0503.



H. OKINETIC™
SHOWERHEADS



see what Delta can do™



Corporate IT Security



Meredith Corporation
Corporate Headquarters
1716 Locust Street
Des Moines, IA 50309

Information Security Statement

The Meredith Corporation information security program has been implemented to enhance Meredith's position as a premier publishing, broadcasting, marketing, and multi-media company. Meredith's corporate information security policy is designed to protect information resources against unauthorized access, disclosure, modification, transfer, storage, misuse, or destruction. This policy is implemented to protect Meredith's privacy and business interests which includes data relating to products, services, marketing, production, financial information, employees, customers, and vendors.



ISO Code of Practice for Information Security

Meredith's information security controls are developed using risk management principles and are guided by the ISO-27002 code of practice for information security. The purpose of this approach is to build information security on a recognized foundation to position Meredith to securely manage data entrusted to Meredith by consumers and business partners. The controls implemented are intended to address requirements identified via risk assessment and contractual obligations. ISO based risk assessments and services agreement reviews are performed across the Meredith enterprise by Meredith IT Security staff, Meredith Internal Audit staff, and external information security partners. As such, Meredith's information security controls include:

- Information security policy – management direction
- Information security organization – governance
- Asset management – protect information assets
- Human resources security – employee on-boarding and off-boarding
- Physical and environmental security – protect computer facilities
- Communications and operations management – manage security controls in systems and networks
- Access control – restrict access rights to networks, systems, applications, functions, and data
- System acquisition, development, and maintenance – build information security into applications

- Information security incident management – anticipate and respond appropriately to information security breaches
- Business continuity management – protect, maintain and recover business-critical processes and systems
- Compliance and privacy – comply with information security policies, standards, laws, and regulations

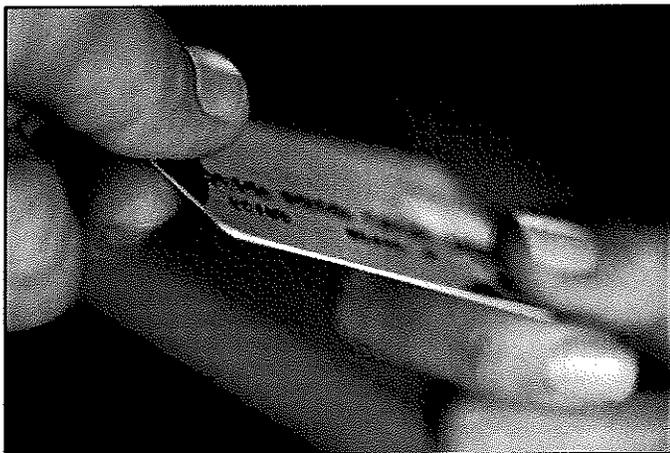
Payment Card Industry Data Security Standard (PCI DSS) Compliance

Meredith Corporation, designated as a PCI DSS Level-3 merchant by Wells Fargo Merchant Services, is required to annually validate compliance with PCI DSS. The PCI DSS consists of security requirements focused on:

- Building and maintaining a secure network
- Protecting cardholder data
- Maintaining a vulnerability management program
- Implementing strong access control measures
- Regularly monitoring and testing networks
- Maintaining an information security policy

Meredith has worked with a PCI QSA (Qualified Security Assessor) and Meredith’s Internal Audit organization to develop the PCI compliant operations, validate ongoing compliance with PCI DSS, report to executive management and the Meredith Corporation Board of Directors. Meredith company officers file Meredith’s AOC (Attestation of

Compliance) with Wells Fargo Merchant Services. Additionally, Meredith IT performs weekly network vulnerability scans assessment on all Internet-facing perimeter systems of Meredith Corporation.



Sarbanes-Oxley Act (SOX) Compliance

As a publically held company, Meredith Corporation complies with the Sarbanes-Oxley Act. On an annual basis, Meredith Internal Audit conducts extensive self-assessments, evaluation, and testing of the internal information technology control policies, procedures, and practices that are included

in SOX Section 404 assessment of internal control. Following the extensive self-assessment, Meredith’s external auditors conduct their independent assessment, evaluation, and testing of internal control policies, procedures, and practices to further ensure that Meredith is compliance with SOX standards. Meredith company officers attest to the establishment, maintenance, and effectiveness of the company’s internal controls including IT controls.

Corporate IT Security, Compliance, and Continuity Team

The Meredith IT Security, Compliance, and Continuity team is responsible for developing, implementing, and maintaining the comprehensive corporation information security policy enterprise wide. The team consists of an information security and compliance function, and a business continuity planning (BCP) and disaster recovery planning (DRP) function.

IT Security & Compliance Function: Design, implement, operate, and maintain the information security program based on the ISO-27002 code of practice controls framework, Sarbanes-Oxley general controls compliance, and PCI DSS compliance for the Meredith Corporation enterprise including Corporate, National Media, Local Media, and Integrated Marketing. Responsibilities include:

- Security policy
- Data classification
- Data leakage protection
- Encryption
 - Data in transit
 - Data at rest (laptops, file shares)
- Awareness training
 - Acceptable Use Policy
 - Information Security
 - PCI DSS
- System protection
 - Anti-virus/anti-malware
 - File integrity monitoring
 - Intrusion detection
 - Vulnerability scanning and remediation
 - Penetration testing
- Security event logging, monitoring, and alerting
- Web content monitoring and protection
- Firewall and router security policy
- Email delivery and receipt
- E-Discovery
- Access control
 - Active Directory access
 - Remote access
 - 2-factor authentication
- Computer security incident response
- Compliance assessments
 - Logical access controls
 - Data center access controls
 - Remote access controls
 - Elevated privilege access
 - Rogue wireless access
 - System configurations
 - ISO code of practice, PCI DSS, SOX IT general controls
- Internal Audit coordination and remediation

Incoming Mail Summary		
Message Category	%	Messages
Stopped by Reputation Filtering	94.3%	62,355,888
Stopped as Invalid Recipients	0.9%	572,262
Spam Detected	0.3%	215,690
Virus Detected	0.0%	411
Stopped by Content Filter	0.1%	78,987
Total Threat Messages:	95.6%	63,223,238
Clean Messages	4.4%	2,922,733
Total Attempted Messages:		66,145,971
Outgoing Mail Summary		
Message Processing	%	Messages
Spam Detected	0.0%	0
Virus Detected	0.0%	0
Stopped by Content Filter	0.1%	593
Clean Messages	99.9%	1,063,976
Total Messages Processed:		1,064,569
Message Delivery		
	%	Messages
Hard Bounces	1.3%	13,578
Delivered	98.7%	1,050,390
Total Messages Delivered:		1,063,968

- Contract, RFP, NDA review



BCP/DRP Function: Design, operate, and facilitate business continuity planning and technology disaster recovery planning program for Meredith Corporation enterprise including Corporate, National Media, Local Media, and Integrated Marketing. Responsibilities include:

- Develop, maintain, and distribute business continuity plans (BCP) and disaster recovery plans (DRP)
- Business recovery exercises
- Technology recovery tests
- Risk assessment and gap remediation
- Emergency notification

Meredith Corporation IT Security Policy Executive Summary

Acceptable Use Policy

Meredith Corporation's computer, electronic, and telephonic communications systems and all communication and information transmitted by, received from, or stored in these systems are the property of Meredith Corporation and, as such, are to be used primarily, if not exclusively, for job-related purposes. While occasional, limited personal use is permitted, this usage should not interfere with regular work duties or create a hostile work environment. Nor should users expect privacy in such usage.

Only authorized computers, software, devices, or equipment may be connected to or installed on Meredith's computers, networks, or communications systems.

Subject to applicable laws and regulations, Meredith reserves the right to monitor the contents of computer, electronic, and telephonic communications including but not limited to telephone, voicemail, facsimile, e-mail, Internet browsing activity, pagers, and digital assistants. Management reserves the right to access, monitor, disclose and/or block all communications for all purposes without notice and without seeking permission. Furthermore, deleted e-mail and files may be restored, retrieved and reviewed by Meredith.

This policy applies to: 1) Company employees, agents, and representatives including consultants, vendors, freelancers, temporary or other workers; 2) all equipment, hosts, or electronic devices connected to any Meredith network.

Any violation of this policy (or poor judgment in complying with these principles) may result in appropriate disciplinary action up to and including discharge from employment or termination of contract, and the exercise of other legal remedies that may be available to Meredith. Violation of these policies may also result in revocation of network access or seizure of equipment.

Meredith's information technology policy can be found in its entirety by viewing the IT Security Policy on Meredith's Intranet site.

Security Policy

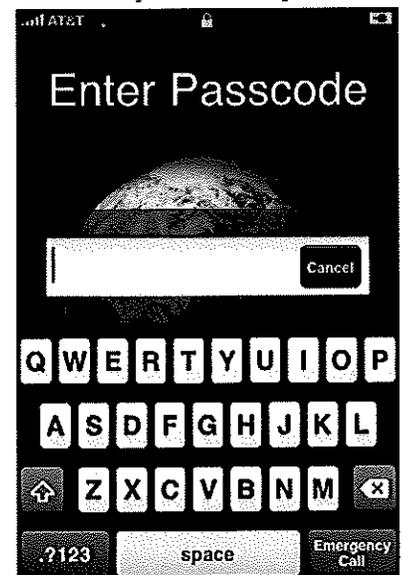
The Meredith Corporation Information Security Policy has been developed to enhance Meredith's position as a premier media and marketing company and is guided by ISO code of practice. Information and the systems that process it are important Meredith resources. This policy is intended to ensure the confidentiality, integrity, and availability of Meredith's information resources.

Meredith's policy is to protect information resources against unauthorized access, disclosure, modification, transfer, storage, misuse or destruction.

This policy applies to all users of Meredith's information resources, regardless of geographic location.

Meredith's executive management (Chairman & CEO, Chief Development Officer & General Council, Chief Financial Officer, National Media Group President, Local Media Group President) is committed to the development and maintenance of an enterprise IT Security program.

The proponents of the Information Security Policy are EVP/Director of Operations and Business Development, Executive Director Information Technology, and Director Corporate IT Security, Compliance, and Continuity.



Organization of Information Security

The Meredith's information security program is centrally managed and coordinated and has been established by executive directive.

Asset Management

IT assets, including hardware, software, network devices, access credentials, information, etc., should be appropriately administered, maintained, and protected. Information has varying degrees of sensitivity and criticality. Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information.

Human Resources

HR responsibilities for information security include performing background checks on potential employees, maintaining employee acknowledgement records for IT Security Awareness Training and Meredith IT Acceptable Use Policy acceptance, and notifying IT personnel of changes in employment status.

Physical and Environmental Security

Meredith facilities should have appropriate physical and environmental controls in place to protect IT assets. Only authorized personnel should be allowed access to designated areas within Meredith facilities.

Communications and Operations

To be effective in managing risk and protecting information resources, Meredith's security policy should include operational procedures, controls, and well-defined responsibilities.

- Third Party Service Delivery: All new extranet connectivity requests will go through a security review.
- System Planning and Acceptance: All servers and network devices on Meredith Corporation networks, whether managed by employees or by third parties, should be built and deployed according to baseline security standards.
- Protection against Malicious and Mobile Code: Technology assets (including workstations, servers, network devices, etc) should be protected against malicious and mobile code.
- Backup: All system and application backups, whether performed by employees or by third parties, should be backed up according to business unit requirements for data recovery.
- Network Security Management: All firewalls and routers and other network devices on Meredith Corporation networks, whether managed by employees or by third parties, should be managed and controlled, protected from threats, and should provide a secure infrastructure for systems and applications using the network.
- Media Handling: Regardless of storage location or whether data is stored on hardcopy or electronic media of any kind, confidential and sensitive data should be stored appropriately, kept only as long as needed, and disposed of properly.
- Exchange of Information: Meredith data shared with third parties should be classified and secured or encrypted appropriately.
- E-commerce Services: Controls should be implemented to protect the information involved in e-commerce.
- Monitoring: Systems should be logged and monitored to ensure that resources are being used properly.
- Vulnerability Management: Network connected technology assets (including workstations, servers, networks devices, firewalls, web servers, etc.) should be periodically scanned for known vulnerabilities. Significant vulnerabilities should be remediated within 30 days or as required by law, contract, or regulatory compliance.



Access Control

Meredith Corporation information should be protected from unauthorized access, modification, disclosure, or destruction whether internally or externally provisioned. Login access to computer systems should be restricted to individuals who need the information to perform their business functions. Users are responsible for all actions that are performed using their login credentials.

Information Systems Acquisition, Development, and Maintenance

Software development/acquisition should incorporate security planning during each phase of software design, testing, installation, or maintenance. Security requirements should be defined based on who will use the system, what data must be secure, what parts of the system execute outside of the Meredith network, and the requirements for user authentication and auditing. Company confidential and sensitive information should be appropriately secured while in transit or in storage using strong encryption methods.

Information Security Incident Management

Meredith IT Security should be notified immediately of any suspected or real security incident or event involving a Meredith computing asset. Investigations into violations of the Acceptable Use Policy of a personal nature must be approved by Meredith Corporate HR or Meredith Corporate Legal.

Business Continuity Management

Business continuity plans (BCP) and technology disaster recovery Plans (DRP) should be developed for all critical operating groups and Information Technology services areas. The plans should be kept up-to-date to reflect changing hardware, software, responsible personnel, and processes. Each operating group or department is responsible for their business continuity plan. Information Technology is responsible for disaster recovery plans for Meredith's corporate systems as well as critical business systems. Selected core plans will be tested annually to ensure that business functions and IT services function reliably and can be maintained during interrupted normal service.



Compliance

Meredith should develop and maintain information security programs that adhere to applicable legal requirements, industry regulations, and company policies pertaining to IT. Examples include: Sarbanes-Oxley requirements (SOX), Payment Card Industry Data Security Standards (PCI), other legislation, and contractual requirements.