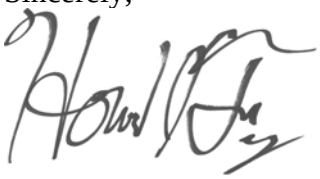
December 21, 2012

Secretary
Federal Communications Commission
445 12th St., SW, Room TW-A325
Washington, DC 20554

Re: In the Matter of Compete, Inc. - "FTC File No. 102 3155"

I hereby submit the attached comments on behalf of the Marketing Research Association (MRA) in reply to the comments of the Electronic Privacy Information Center ("EPIC") regarding the Matter of Compete, Inc. (FTC File No. 102-3155).

Sincerely,



Howard Fienberg, PLC
Director of Government Affairs
Marketing Research Association (MRA)

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org

Reply Comments of the Marketing Research Association
To
The Federal Trade Commission
In the Matter of Compete, Inc.
"FTC File No. 102-3155"

Table of Contents

1. Introduction

The Federal Trade Commission ("the Commission") proposed a consent agreement with Compete, Inc. on October 29, 2012[1] to settle alleged "charges that it violated federal law by using its web-tracking software that collected personal data without disclosing the extent of the information that it was collecting [and] allegedly failed to honor promises it made to protect the personal data it collected."[2] The Electronic Privacy Information Center ("EPIC") submitted comments[3] on November 19, 2012 in response to the agreement.

The Marketing Research Association ("MRA") now files these comments in response to the comments of EPIC. MRA, a non-profit national membership association, is the leading and largest association of the survey, opinion and marketing research profession[4] in the United States. MRA promotes, advocates and protects the integrity of the research profession and strives to improve research participation and quality.

EPIC urged the Commission "to (1) strengthen the Order by requiring Compete to implement Fair Information Practices similar to those contained in the Consumer Privacy Bill of Rights; (2) make Compete's independent privacy assessments publicly available; (3) clarify the scope of implicit deception in the context of privacy policies; and (4) develop a best practices guide for anonymization techniques."[5]

---

[1] Compete, Inc., Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 65,550 (proposed Oct. 29, 2012), http://www.gpo.gov/fdsys/pkg/FR-2012-10-29/pdf/2012-26464.pdf

[2] "Tracking Software Company Settles FTC Charges That it Deceived Consumers and Failed to Safeguard Sensitive Data it Collected." Federal Trade Commission press release. October 22, 2012. http://www.ftc.gov/opa/2012/10/compete.shtm

[3] Comments of the Electronic Privacy Information Center In the Matter of Compete, Inc.; FTC File No. 102 3155. November 29, 2012. http://www.ftc.gov/os/comments/competeconsent/00004.html

[4] The research profession is a multi-billion dollar worldwide industry, comprised of pollsters and government, public opinion, academic and goods and services researchers, whose members range from large multinational corporations and small businesses to academic institutes, non-profit organizations and government agencies.

[5] Comments of EPIC. Page 2.

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org

MRA's comments are filed in support of the entire research profession. Because Compete is a research company, we are concerned that the changes to the Compete order sought by EPIC would pose a potential threat to all research companies in the U.S.

2. The Commission's complaint

According to the Commission, consumers downloaded tracking software from Compete, a survey, opinion and marketing research company. "Once installed, the Compete tracking component operated in the background, automatically collecting information about consumers' online activity. It captured information consumers entered into websites, including consumers' usernames, passwords, and search terms, and also some sensitive information such as credit card and financial account information, security codes and expiration dates, and Social Security Numbers."[6] The Commission "charged that several of Compete's business practices were unfair or deceptive and violated the law," such as failing "to disclose to consumers that it would collect detailed information such as information they provided in making purchases," not just web pages the consumers visited.[7] The Commission also alleged that "Compete made false and deceptive assurances to consumers that their personal information would be removed from the data it collected."[8] After contending to consumers that "All data is stripped of personally identifiable information before it is transmitted to our servers" and "We take reasonable security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal information," the Commission alleged that "Compete failed to remove personal data before transmitting it; failed to provide reasonable and appropriate data security; transmitted sensitive information from secure websites in readable text; failed to design and implement reasonable safeguards to protect consumers' data; and failed to use readily available measures to mitigate the risk to consumers' data."[9]

3. The Commission's consent agreement with Compete

The consent agreement proposed by the Commission requires "Compete and its clients to fully disclose the information they collect and get consumers' express consent before they collect consumers' data in the future. In addition, the settlement bars misrepresentations about the company's privacy and data security practices and requires that it implement a comprehensive information security program with independent third-party audits every two years for 20 years."[10]

4. Deception by omission

EPIC supported "the Commission's finding of deception by omission" in the Compete case[11] and further called for the Commission to "amend its Deception Policy to explicitly categorize omissions impacting consumer privacy as deceptive under Section 5 [of the FTC Act].[12] This

[6] FTC press release.
[7] FTC press release.
[8] FTC press release.
[9] FTC press release.
[10] FTC press release.
[11] Comments of EPIC. Page 6.
[12] Section 5 of the Federal Trade Commission Act (FTC Act), Ch. 311, §5, 38 Stat. 719, codified at 15 U.S.C. §45(a).

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org

clarification will inform companies that they must notify consumers of all privacy policy changes, and that failure to do so will result in a finding of deception under Section 5."[13]

The Commission currently finds deceptive omissions to be material "if they significantly involve health, safety, or other areas with which the reasonable consumer would be concerned."[14] Such a finding might be applicable to scenarios regarding data security protections for personally identifiable information subject to criminal abuse (e.g., credit information that could lead to identity theft) or other tangible harm.

While some survey, opinion and marketing research indicates that consumers, on average, are concerned about their privacy, and EPIC shared that "studies prove privacy is important to consumers,"[15] notifying consumers of every minute privacy policy change could work counter to the interest of actually informing consumers, since over-notification and excessively lengthy privacy policies already may be causing consumers to stop paying close attention to their own privacy needs and wants and growing more careless in how they handle their own privacy. Therefore, MRA would be opposed to the proposed explicit categorization of omission as a deception under Section 5.

5. De-identification

EPIC's comments on companies' claims to "anonymize or de-identify personal information by aggregating it or assigning pseudonyms to it"[16] run up against an ongoing debate in the academic and policy spheres on whether or not data can ever be fully de-identified or anonymized. If it cannot, then pretty much any piece of data is ultimately personally identifiable.

Speakers at a conference in Washington, DC in December 2011 clashed extensively over this very question.[17] Several researchers, like Latanya Sweeney, Director of the Data Privacy Lab at Harvard University, contended that most any data could be re-identified, based on a pair of her studies. Several other researchers responded that the two biggest re-identification studies were very limited cases and not generalizable.[18]

To illustrate the debate, consider a data point such as date of birth, which could be considered personally identifiable because it splits the population into 25,000 cells and can enable re-identification. If you combine such data with a zip code containing only a handful of people in a certain age range, it may be very easy to re-identify. Professor Peter Swire of Ohio State University made an analogy at the conference to a cop collecting clues. A suspect is male, tall, with red hair. That would not be enough to re-identify, but it would certainly make it easier. It is more a matter of how much legwork, analysis and extra data is available and

[13] Comments of EPIC. Page 7.
[14] "FTC POLICY STATEMENT ON DECEPTION." Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984). at http://www.ftc.gov/bcp/policystmt/ad-decept.htm
[15] Comments of EPIC. Page 7.
[16] Comments of EPIC. Page 8.
[17] "Personal Information: The Benefits and Risks of De-Identification." A conference held by the Future of Privacy Forum (FPF) on December 5, 2011. http://www.futureofprivacy.org/2011/10/19/upcoming-fpf-event-one-day-conference-dec-5/
[18] FPF Conference.

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org

accurate. That is what weighs against the public being able to re-identify de-identified data, according to Professor Swire.[19]

Khaled El Eman, a researcher at the University of Ottawa, felt that the data re-identification efforts by Sweeney and company were the exceptions that prove the rule. Most attacks fail miserably, he said. According to Eman, the studies that succeeded are too small, too few, too ambiguous, too heterogeneous and with confidence intervals that are way too large. Eman concluded that, "Re-identification is hard." He suggested that there would need to be 40-50 replicable studies to start to change such a conclusion.[20]

It is also important to remember that de-identification carries costs as well as benefits. Daniel Barth-Jones, epidemiology professor at Columbia University, warned at that conference that excessive de-identification of data can yield huge statistical errors and inaccurate research results: the greater the level of de-identification, the less statistically useful the data becomes.[21] Blanket de-identification could grind statistical research and number-crunching to a standstill. Ultimately, is there a point in de-identification to a level where there are significantly easier and cheaper ways of getting the data? Professor Barth-Jones ended his presentation with a warning about trade-offs, that the real harm is not the ephemeral threat to privacy but the real threat of "not catching the next HIV epidemic".[22]

EPIC noted in their comments that, "Given the problems associated with certain de-identification techniques, and the falsity of claiming that pseudonyms and aggregation necessarily render data anonymous, the Commission should issue a best practices guide to de-identification… greater clarification and standardization is needed."[23]

There may be benefit to engaging the Commission in the broader public debate over de-identification. It is not at all clear, however, that a Commission-issued "best practices" would advance the debate at this point.

6. Implementing the Fair Information Practices

EPIC commented that the Commission's consent agreement with Compete[24] should advance the President's Consumer Privacy Bill of Rights proposal[25] by "adhering to additional Fair Information Practices"[26] such as requiring that consumers be able to "exercise individual control over which types of information Compete intends to collect and disclose…. the Order should permit Compete consumers to select which data Compete will collect and for what purposes Compete can disclose consumer data. As the Order is currently written, Compete simply informs consumers of the type of information it will collect; it does not permit

[19] FPF Conference.
[20] FPF Conference.
[21] FPF Conference.
[22] FPF Conference.
[23] Comments of EPIC. Page 9.
[24] Compete order.
[25] White House, "CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY." February 2012. Available at http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf
[26] Comments of EPIC. Page 12.

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org

consumers to decide which information Compete collects."[27] EPIC's comments also lament that, "the Order does not grant consumers a right to access and ensure accuracy of the data that Compete maintains."[28]

MRA already requires that researchers seek tailor-made approaches to transparency with regard to clients, research participants, and the public at large[29] that are appropriate to different modes and methods of research. Research best practices require disclosure of what data is being collected and used, and for what purpose, and that participants be given the opportunity to opt out. Given that EPIC's stated concerns focus on the sharing of data for advertising purposes,[30] the proposed broad application of consumer control over research use of data does not make sense. In particular in such a case, research codes and best practices forbid the use of personal information from research studies for direct marketing and advertising back to research participants.

The principle that consumers should be able to access and correct data on themselves is common to multiple bills currently in Congress,[31] as well as the Commission's own recent Privacy Report,[32] so it should be no surprise that EPIC would seek the same from the Commission in this Order. Such a demand of access to consumer data may make sense in contexts where such data (particularly if inaccurate) could adversely impact a consumer's credit rating, personal or professional reputation, or likelihood of becoming a victim of identity theft or fraud. However, none of these conditions should reasonably be assumed to apply to survey, opinion and marketing research data. Participation in survey, opinion and marketing research is voluntary.

The cost of access and correction could potentially be quite onerous, especially for smaller research companies and organizations, given a potential deluge of frivolous or pointless inquiries. Since the research process is interested in broad groups, not individuals, compiling and tracking individual consumer data, by the individual, would require complex and expensive procedures and infrastructure not currently in use. Moreover, such tracking could lead to a much greater threat of harm from data leakage and empower the kind of consumer

[27] Comments of EPIC. Page 12.
[28] Comments of EPIC. Page 12.
[29] For instance, in the MRA Code, Part A of the Preface describes the purpose of code in providing fairness, confidence in research, and ethics towards research participants. In the Code itself, item 3 requires disclosures for public-release research; item 7 requires that research be reported accurately and honestly; item 12 forbids researchers from misrepresenting their qualifications and experience; item 21 forbids representing a non-research activity to be research; item 25 requires that research participants are informed at the outset if interviews/discussions are audio/video recorded; item 31 demands that researchers make factually correct statements, whether verbal or written, to secure cooperation and honor promises made during the interview to research participants; item 54 requires researchers to provide access to their privacy policies; and item 55 obliges researchers to provide participants the choice with each survey to be removed (opt-out) from future Internet invitations. Available at http://www.marketingresearch.org/the-code-of-marketing-research-standards-0
[30] Comments of EPIC. Page 11.
[31] These include several data security bills, Rep. Bobby Rush's Best Practices Act (H.R. 611), and Sen. John Kerry's Consumer Privacy Bill of Rights Act (S. 799).
[32] Federal Trade Commission. Protecting Consumer Privacy in an Era of Rapid Change. March 2012. Available at http://ftc.gov/opa/2012/03/privacyframework.shtm

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org

tracking that concerns both EPIC and the Commission (such as in the consent agreement with Compete).

The ability of companies to authenticate the identity of consumers requesting access is another serious concern. That kind of authentication would require collecting and checking even more data, which runs counter to EPIC and the Commission's interest in data minimization and limited data retention.[33] Plus, necessary authentication procedures and processes would add to the cost in money and time on the part of research organizations.

MRA supports the concept of a "sliding scale" for access and correction responsibilities in order to reconcile the vague benefits with the expected costs. We propose that the availability and extent of access should depend on the data actually being susceptible to use for criminal or fraudulent purposes.

The Commission pointed out in its Privacy Report that, "the extent of access should be proportionate to the sensitivity of the data and the nature of its use."[34] To that point, MRA stresses that the use of the data should matter, and survey, opinion and marketing research data should, in most cases, not be subject to access, especially given that consumer concern focuses on commercial data brokerage for marketing and credit purposes, not on research. MRA particularly wishes to avoid a steep slippery slope where most any kind or combination of data could be tied to a supposedly adverse outcome.

7. Making the privacy audits public

EPIC maintained in their comments that, "to facilitate public education and the transparency of the audit process, the Commission should make Compete's privacy audits publicly available."[35] EPIC has not made a reasonable case for why audits should be publicized. The case that "similar audits containing extensive technical details have been released in their entirety, all without identifiable competitive harm" is not made because the support relies on references to non-research-related foreign cases[36] and identifying the "competitive harm" would likely require a sizeable window of close study.

These privacy audits will contain plenty of trade secrets and delicate information. There are broader implications to making such information public, particularly for the survey, opinion and marketing research profession. It could potentially interfere with core research processes, such as the classification of information, impair the overall performance of research and hurt

[33] That does not mean that MRA supports the Commission getting involved in data minimization regulations for survey, opinion and marketing research. As a broad principle, not collecting or maintaining more data than necessary to fulfill a certain purpose makes sense. However, within various modes and methods of research, the need to retain data will vary, and should be properly subject to those needs, not an arbitrary decision by a regulatory body unfamiliar with the processes and practices of research. Additionally, a major objective of research is to understand attitudes, behaviors and opinions over time. The collection and analysis of this information often leads to new theories over time, requiring the re-visiting of older data. Prescribed retention periods would thus diminish the long-term value of data collected for research purposes.

[34] *Ibid*.

[35] Comments of EPIC. Page 13.

[36] Comments of EPIC. Page 13.

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org

the research business. Therefore, MRA does not support making public the privacy audits in the consent agreement.

8. Conclusion

For the reasons explained, MRA urges the Commission to reject the additions to the Compete consent agreement requested by EPIC.

Marketing Research Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545 • Fax: (888) 512-1050
Website: http://www.marketingresearch.org