WRITTEN TESTIMONY OF

FRANK CASERTA

CHIEF SECURITY OFFICER

ACXIOM CORPORATION

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

HEARING ON "DATA BROKERS – IS CONSUMERS'

INFORMATION SECURE?"

NOVEMBER 3, 2015

Chairman Flake, Ranking Member Franken, distinguished Members of the Committee, my name is Frank Caserta and it is my pleasure to represent Acxiom at today's proceedings. I am the Chief Security Officer for Acxiom Corporation, a role that I have held for the past 12 years.

Acxiom's business consists of two main parts: first, large scale computer processing services, including more recently specialized services to enable our clients to reach their marketing audiences via mobile, television and online, which we refer to as our "digital reach service;" and second, information products – what Capitol Hill would consider the "data broker" business. We help our clients successfully manage information regarding audiences they wish to reach, connect with these audiences, personalize experiences with their customers and create relationships that bring both them and their customers greater benefits. Our role is sourcing and analyzing the data they collect.

Because we are all about data, Acxiom well understands that we have an inherent responsibility to safeguard the personal information we process for our clients and the information we bring to the market. Therefore, we work within our industry and across the commercial spectrum, as well as with federal, state, and international governments to develop and implement best practices for the collection, use, and protection of data. We have been recognized for our efforts to meet and exceed the guidelines of the Digital Advertising Alliance, Interactive Advertising Bureau, Mobile Marketing Association and Direct Marketing Association, among others. We limit the use of our data depending on the type of data and the permissions associated with that data. And, we are proud to be the first and only information services company to offer consumers online access to and control of marketing data, which we do through our web portal, www.AboutTheData.com.

About Acxiom Corporation

Acxiom was founded in 1969 in Little Rock, Arkansas. We are headquartered there, with operations throughout the United States, including in California, Illinois, New York, Ohio, Tennessee, and Texas. The company also has offices in eight countries across Europe and Asia. From a small startup company in Arkansas, Acxiom Corporation has grown into a publicly traded corporation with some 4,000 employees worldwide.

Acxiom's U.S. business includes two distinct components: our large scale computer processing services, which includes our digital reach service, and a line of information products. Acxiom's computer services represent over 80% of the company's business and include a wide array of leading technologies and specialized services focused on helping clients manage their own customer information. These services would include things such as ensuring accurate name, address, and contact information; and analytics to help companies gain insights into their customers to improve their offerings. Our digital reach service enables our clients to reach marketing audiences across all digital channels. These services are offered to clients whom we carefully screen – primarily large businesses, not-for-profit organizations, political parties and candidates, and government agencies. Acxiom's private sector computer services clients represent a "who's who" of America's leading companies and include 49 of the Fortune 100. Acxiom helps these clients improve the loyalty of their customers and increase their market share, while reducing risk and assisting them with their compliance responsibilities under state and federal law. Finally, Acxiom helps government agencies improve the accuracy of the

personal information they hold.

The balance of Acxiom's business comes from information products. Our information products are comprised of three categories: fraud management products, telephone directory products, and marketing products. These products each play a unique role, helping to fill an important gap in today's business-to-consumer relationship and support three channels: online, mobile and addressable television. Our information products represent less than 20 percent of the company's total business.

Acxiom's fraud management products are sold to companies and government. These verification services validate that a person is who he or she claims to be.

Acxiom's telephone directory products include name, address and published telephone information. This information is compiled from the white and yellow pages of published U.S. and Canadian telephone directories and from information available from the various directory assistance services provided by the telephone companies. This information enables businesses and consumers to locate other businesses or consumers and powers many of the web white and yellow page services.

Acxiom's marketing information products provide demographic, lifestyle, and interest information to companies to reach prospective new customers who are most likely to have an interest in their products and to better understand and serve the needs of existing customers. They are compiled from publicly available data, from public records, from surveys and from summarized customer information where appropriate notice and choices has been provided.

Providing a means to verify identity and protect access to personal information, Acxiom's fraud management and risk products provide an obvious benefit to the public. Often less obvious is the value the public enjoys from marketing data. According to a study for the Digital Marketing Association undertaken by professors from the Harvard School of Business and Columbia University, the Data-Driven Marketing Economy (DDME) added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in 2012 alone.[1] Competition resulting from the DDME is forcing companies to be less focused on their product and more focused on consumers. With the DDME, companies must now actively seek to determine consumer needs and provide tailored options. Gone are the days, in the words of Henry Ford, when customers could have any color car they wanted, so long as it was black.

To understand the critical role Acxiom plays in facilitating the nation's economy and safeguarding consumers, it is also important to understand what the company does not do. Acxiom does not maintain one big database that contains detailed information about all individuals. Instead, the company develops discrete databases tailored to meet the specific needs of Acxiom's clients – entities that are appropriately screened to assure they are legitimate and have a legitimate purpose for the data, and with whom Acxiom has legally enforceable contractual commitments. Acxiom does not provide information on individuals to the public, with the exception of our telephone directory product.

[1] John Deighton and Peter Johnson, *The Value of Data: Consequences for Insight, Innovation, and Efficiency in the U.S. Economy*, Oct. 8, 2013, available at: http://ddminstitute.thedma.org/files/2013/10/The-Value-of-Data-Consequences-for-Insight-Innovation-and-Efficiency-in-the-US-Economy.pdf.

Our Commitment to the Ethical Use of Data

At Acxiom, we take data security very seriously. We have a longstanding tradition and engrained culture of protecting and respecting consumer interests in our business. We recognize that we have a responsibility to safeguard the personal information we hold and process on behalf of our clients and that we collect for our information products. To that end, the company is today, and always has been, a leader in developing self-regulatory guidelines and in establishing security and privacy policies and practices. For the 46 years we have been in business handling data, Acxiom has focused on assuring a safe environment for the information. We have in place a Security Oversight Committee that is headed by a Chief Security Officer with more than 30 years of IT experience, and we were the first company in the world to have a Global Privacy Executive position named in 1991.

Our Commitment to Security

All industries within the private sector, whether they be small or large, utilities, healthcare, financial, information, or anything else, must confront growing cyber-threats to systems. For data-intensive companies, these threats are a natural impetus to constantly evolve and strengthen cybersecurity. Systems protection for these companies is not only a matter of risk to customers, but also risk to crucial business assets. Quite simply, being all about data means being all about security.

Data-brokers in general, like most consumer-facing companies subject to Federal Trade Commission regulation, are required to employ "reasonable" security measures to protect systems and information. Each company must figure out what constitutes "reasonable" security based on the unique threats they face. The resulting plans companies develop from that analysis are necessarily confidential to protect companies' security. As such, we are happy to characterize the general parameters of Acxiom's security program. However, we will avoid today providing details that could compromise our security posture, and we are not in a position to comment on other companies' internal, confidential security measures. As a matter of good security, we would not have detailed information on what they do.

Broadly speaking, our security program is designed to exceed federal requirements for safeguarding data. We are often a leader in adopting new security techniques and protocols for the protection of data. As an example, even though Acxiom's marketing information products are not covered by the Gramm- Leach-Bliley Act (GLBA), we nevertheless apply GLBA Safeguard Rule to those products. Ultimately, Acxiom's approach to information security goes beyond what is required by either law or self-regulation.

Our commitment to security also comes from our first-hand experience with data breaches. In 2003, the passwords on a server that resided outside our main system firewalls were hacked and many of the lists transferred by the server stolen. Acxiom used this server to transfer marketing lists between Acxiom and our clients. While marketing lists usually do not contain sensitive data, our standard protocol was to encrypt any sensitive data on these files, so no consumer was harmed by the incident. We were also fortunate that the collective efforts of Acxiom and law enforcement resulted in apprehending and bringing to justice the criminals involved in this breach. From this experience, we learned a lot about both the risks that companies face as well as

how to effectively work with the authorities when such incidents occur.

It takes a constant state of vigilance to stay ahead of the security challenges in today's world. We make frequent changes to improve our security measures and practices. Acxiom must have comprehensive policies governing the security of our operations. These policies must be backed with effective governance that will assure adequate measures are taken for protection.

Acxiom's governance model includes many key elements. Acxiom has named executive positions for Security, Privacy, Audit, and Risk. They are responsible for policies, strategy, and programs globally. They are accountable to the Executive Committee that leads Acxiom and also to the Acxiom Board of Directors.

Acxiom makes use of security industry standards that include ISO 27000, NIST, PCI, FISMA, and HITRUST. These standards are essential for identifying and managing security risks. They also provide taxonomy for discussion and comparison between different stakeholders such as clients and service providers.

Our security assurance and audit programs span internal audits, external independent audits, client audits, and supplier assessments are all designed to provide customers and management with a level of assurance that effective security controls are in place and working as intended. Here are some key assurance highlights:

- **Annual Audits –** Acxiom contracts with an outside auditor to perform an annual audit according to industry audit standards (specifically SOC 2, Type II, per the SSAE 16 standard) and in compliance with Sarbanes-Oxley Act Section 404.
- **Vulnerability Testing –** Acxiom contracts with a reputable third-party to perform quarterly penetration and vulnerability testing.
- **Third-Party Certification –** Acxiom is compliant on client-dedicated environments requiring PCI third-party certification.
- **Numerous Client Audits –** Acxiom undergoes approximately 50 client audits per year. These are conducted onsite at Acxiom by clients or their designated third-parties.
- **Client Questionnaires –** Acxiom completes approximately 250 questionnaires a year, on behalf of our clients, which drill into our security capabilities to determine their comfort level with our ability to protect data, systems, and networks.

Acxiom's security programs, as defined by our information security policy, provide for many layers of defense. The following is a general description of a few of the key security elements:

- **Network Security –** Zoning for defense, limiting access to systems and data, segregating data and clients, limiting breach exposure, and providing intrusion detection.
- **Security Training and Awareness –** Security and privacy policy training for all associates and contractors as well as in depth training and certifications for security staff.

- **Data Security –** Encryption, limited access, data loss prevention, and network segmentation.
- **Product Life Cycle Management –** Privacy impact assessments, security risk assessments, architecture review, secure coding, security testing, vulnerability scanning and penetration testing.
- **Configuration, Change, and Patch Management –** Maintaining security of systems and applications until decommissioned.
- **Antivirus and malware management –** Keeping malicious software off of systems and networks.
- **Log Management –** Logging key application and systems events, retaining and monitor for anomalies.
- **Event and Incident management –** Detecting security events and responding with established incident response protocols (contain, remediate, and report as required).
- **Data Center Controls –** Isolated data center facilities with limited access that provide critical environmental supports.
- **Human Resource Controls –** Standards for employment and access, and security clearances where required.

No security program can claim to be perfect. Even our nation's security agencies have recent incidents proving that. But security can be constantly vigilant.

In addition to security programs and controls, Acxiom believes it is prepared to handle a security breach in the event that it does occur. We have documented incident response plans. We train key personnel every year on security incident response, crisis communication, and disaster recovery. We conduct mock incident exercises to make sure the processes will work when needed. These programs can limit loss and exposure as well as make sure we comply with all the appropriate notification and response requirements that are covered by law and by client contracts.

Mr. Chairman, Acxiom appreciates the opportunity to participate in this hearing today and to assist Congress in identifying how to best safeguard the information. Acxiom is available to work with the Committee on any requested additional information.