WRITTEN TESTIMONY OF

JENNIFER BARRETT-GLASGOW
GLOBAL PRIVACY OFFICER
ACXIOM CORPORATION

BEFORE THE
UNITED STATES HOUSE
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

HEARING ON "WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?"

JANUARY 27, 2015

Chairman Burgess, Ranking Member Schakowsky, distinguished Members of the Committee, thank you for holding this hearing and taking the time to address much needed federal legislation with regards to data security and data breach notification. I am very pleased to be here today, and Acxiom appreciates the opportunity to participate in this hearing and the overall discussion surrounding these issues.

Acxiom's business consists of 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 several information products. We help our clients successfully manage audiences they wish to reach, connect with these audiences, personalize experiences with their customers and create profitable customer relationships by sourcing and analyzing the data they collect.

Acxiom 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 it is 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 a 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 5,500 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 computer 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 so they can improve their offerings. Our digital reach service enables our clients to reach marketing audiences across all digital channels. These services are offered primarily to 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.

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 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.

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 – the position I have held since its inception in 1991.

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. Furthermore, 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.

We have long been a leader in data stewardship, consumer education and transparency. Acxiom believes in giving consumers a voice and a choice. And while we've long offered consumer access and correction to our Fraud and Risk data products, we recognized the need to become even more transparent with our marketing information products. In 2013 we launched the first-of-its-kind marketing data access portal, www.AboutTheData.com. This is a website where consumers can log in and see what information Acxiom has gathered about them that is used for marketing purposes. Once there, consumers can update, modify and delete the information, and of course opt out from Acxiom's marketing data products altogether. This site also hosts information that educates consumers on how marketing data is used and why this use might be of value to them. This type of consumer voice and choice over marketing data, we believe, should be the industry standard. To date, about 750,000 people have visited the portal, approximately 16% have edited one or more data elements about themselves and less than 3 percent of visitors have opted-out. Acxiom was the first to offer this type of transparency, and we remain the only marketing services company to do so at present.

We have not stopped there. More recently Acxiom has partnered with the Better Business Bureau to help launch their Digital IQ initiative to broaden consumer's knowledge on the use of data and help consumers develop skills for effectively navigating the digital world. Many consumers do not have a good understanding of how data is collected and used. We feel a responsibility – and believe it is a good business practice – to help them understand. We have also recently announced our own initiative, AcxiomData4Good. This initiative makes data accessible and actionable for charitable organizations to better deliver value and service to consumers and the community at large. This program leverages Acxiom's leadership in marketing data and analytics, along with our technology assets and talent, to improve and hopefully solve pressing community issues in the areas of health, education and humanitarian aid.

Finally, we have recently awarded a grant to fund the efforts of the Information Accountability Foundation to develop an operational Unified Ethical Framework that business and other organization can use to apply ethical governance to the use of marketing data.

Acxiom Supports Effective Federal Legislation

The recent data breaches of large companies have once again highlighted the importance of data security and breach notification legislation. Acxiom testified before this Committee almost 10 years ago advocating for federal legislation on data security and breach notification. Since then, the frequency and severity of breaches has increased substantially.

This Committee has invested significant time and energy over the past 10 years debating and passing multiple breach notice bills, but unfortunately Congress has been unable to enact any such legislation into law. In the interim, almost every state has enacted its own breach notice law, resulting in a web of varying and even conflicting requirements that are subject to frequent change by state legislatures.

This complex array of laws and regulations continues to fuel Acxiom's strong support for preemptive federal legislation, providing both a ceiling and a floor, which benefits both businesses and consumers. Businesses would gain the benefit of more easily managed and understood compliance obligations, as well as increased regulatory certainty. There have been many formulations of preemption language over the years. One we would commend to the Committee is the following:

> *No law, rule, regulation, requirement, standard or other provision having the force and effect of law relating to data security or notification following a breach of data security may be imposed under State law or the law of a political subdivision of a State on a person subject to this Act.*

From the consumer's perspective, a single federal standard not only increases their confidence in the safeguards protecting information businesses hold, but also makes notice procedures in the event of a breach clearer. It has been discussed many times before this Committee, but there is indeed a danger of over-notification – that consumers will not pay attention to a notice that matters because they have previously received notices under circumstances where they were not at risk. Therefore, Acxiom supports a harm-based trigger for notification.

We also support a reasonable timeframe for the notice, such as one that requires notice "without undue delay." An unduly short or specific statutory deadline may not provide enough time for companies and law enforcement to sufficiently investigate a breach in a manner that allows them to identify the means and extent of the breach, and gives law enforcement sufficient time to identify the perpetrators. Acxiom also supports the type of extension mechanism the Energy & Commerce Committee has included in many breach notice bills over the years. If a law enforcement agency determines that notification would impede an investigation, notice can be delayed. The Administration's recent data breach notification proposal limits this delay to instances where it is requested by a federal agency; the Energy and Commerce Committee's broader language from previous bills is better.

We would like to highlight one other distinction between what the Energy & Commerce Committee historically has supported in data breach notice legislation and the President's proposal. The President's proposal includes an exemption from notice if a risk assessment shows there is "no reasonable risk" that the breach will result in "harm." The breached entity is required to conduct a risk assessment to determine absence of a reasonable risk of harm. Failure to conduct the risk assessment reasonably, or in accordance with generally accepted standards, is itself a separate violation of law. By contrast, previous Energy & Commerce bills do not create an additional possibility of violation of law. For notice to be determined to be unnecessary, the breached entity would need to determine that there is no reasonable risk of "identity theft, fraud, or other unlawful conduct" – harms that are cognizable under law. Practically, this would necessitate a risk assessment, However, this approach does not make an improper risk assessment – which could be inadvertent – a separate violation of law. Among the specific Energy & Commerce bills to which we are referring on this provision is H.R. 2221 from the 111th Congress, sponsored by the former Chairman of this subcommittee Mr. Rush and passed with bipartisan support. More recently this type of approach has been in Vice Chairman Blackburn's legislation.

Acxiom also supports effective security measures. Acxiom believes it is likely to meet any reasonable security requirement. As part of our clients' due diligence processes, our security is assessed and audited upwards of 80 times per year. This is in addition to our own internal audits. Through this collaborative process we have significantly grown our technical knowledge and expanded our security measures. However, perfect security simply does not exist. As the President noted in announcing his recent proposal, "[E]ven as we get better, the hackers are going to get better, too." Given the need to constantly adapt security tactics, we recognize that security requirements should not be legislated with too much specificity. Therefore, we advocate for flexible measures that set a flexible baseline for security such as applying the Gramm-Leach-Bliley Act Safeguards Rule to everyone.

Acxiom believes that businesses have a responsibility to educate their employees about security risks and that government has a role to play in educating the public in general on these topics. Over the years, we have seen the intended use of information taken in a data breach expand from credit card and identity theft to very sophisticated scams based on the personal data that is stolen. We can collectively protect the American public better if individuals are more aware of these kinds of crimes and can be more vigilant about recognizing when they may be the target of such scams.

Our constant goal is to live up to the responsibility we have to safeguard personal information. In addition to state and federal laws, we are subject to industry guidelines and compliance directing that transparency is provided to consumers when the data was collected. Federal preemptive data security and breach notification legislation such as we recommend would bring greater regulatory certainty to Acxiom and other businesses. Most important, such legislation would give greater confidence to consumers about the safety of their personal data.

It is Acxiom's understanding that the Committee intends to keep this bill focused on breach notice and data security. We believe that is the right decision. Over the years, the enactment

prospects of data breach notification and security bills have been hampered by the inclusion of "privacy" provisions for which there is less consensus. In particular, various bills have included so-called "data broker" provisions, such as requirements that data brokers allow consumers to access and correct information about them, or to opt-out of use of information about them for marketing purposes. As I have mentioned, Acxiom already does and will continue to do these things. However, the bills invariably have pulled in hundreds, perhaps thousands of companies who do not consider themselves to be "data brokers," which has generated opposition to bills that largely have had consensus support for the remainder of their provisions – at least the thrust of those provisions, if not the precise legislative language. There are plenty of important issues to debate regarding data, but we believe Congress will best serve the public by maintaining this bill as a breach notice and security bill, and addressing other issues separately to see if a consensus can develop around them.

Mr. Chairman, Acxiom appreciates the opportunity to participate in this hearing today and to assist Congress in identifying how to best safeguard the nation's information. Acxiom is available to provide any additional information the Committee may request.