WHY DATA GOVERNANCE MATTERS NOW, MORE THAN EVER – AND WHAT TO DO ABOUT IT

THE VITAL ROLE OF TRUST IN OUR DATA-DRIVEN ECONOMY

The impact of consumer data on the economy is massive. It's vital to the success of ad-supported internet businesses, which in 2016 contributed over $1.1 trillion to the US economy and supported over 10 million jobs. And this is just one of the many areas where data plays an important role in driving economic value.

As the world becomes data-driven, the businesses with the best ability to access and use data will be in the strongest position to win over time. This stands to reason – data is critical for optimizing how budgets are spent and essential for powering the personalized experiences that consumers crave.

Research shows that trust is the primary factor that determines when a consumer is willing to share data with a business. Consequently, trust has become the most powerful currency in business today. And to develop trust, organizations must invest appropriately in data governance and stewardship programs.

Sheila Colclasure

Sheila is Acxiom's Chief Privacy Officer and Global Executive of Privacy and Public Policy. In 2017, Sheila was selected to participate in the prestigious Presidential Leadership Scholars program.

Frank Caserta

Frank is Acxiom's Chief Security Officer. Frank has been leading security and data protection for Acxiom for over 14 years.

This includes two parallel disciplines - making sure data is protected through appropriate security controls and making sure data use is ethical. Applied data ethics, or Ethics by Design, is essential to ensure data use is legal, just, and fair to consumers. This is critically important for actively shared data, but even

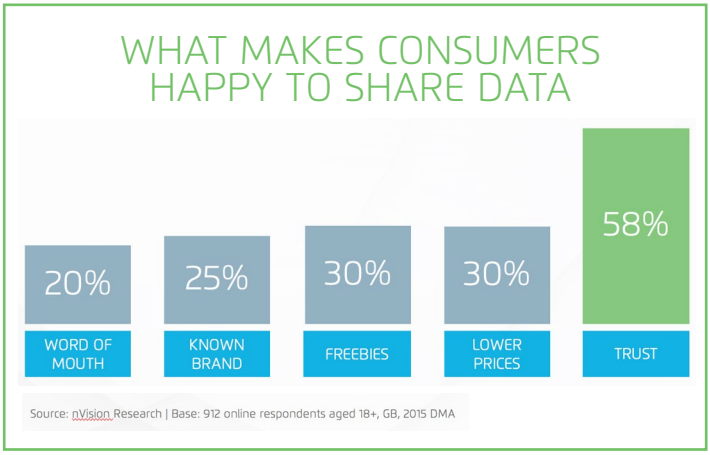
more important as we accelerate into a world of observational data and passive collection.

These are exciting times for marketers. The opportunity to engage consumers with relevant brand experiences based on their immediate context has never been greater. The pace of innovation is accelerating. The Internet of Things (IoT) is here. Connected devices, from our cars to our smart TVs include embedded sensors. Everyone and everything is generating data, creating an explosion of new data types at unprecedented volumes. More companies than ever are monetizing their data assets and forming partnerships to combine data with others in a privacy-compliant way.

The regulatory landscape is also evolving quickly. The new pan-European General Data Protection Regulation (GDPR) will come into force May 2018. GDPR is a game-changing law that impacts any business with European data centers or audiences. It requires accountability when a company controls data or processes it on behalf of others, and it gives individuals more data protections and privacy rights than ever before.

GDPR is part of the Digital Single Market regulatory package, an acknowledgment that economies are becoming digital, depend on data to function, and require data protection that addresses inevitable and complex digital data flows. There are concerns that the new law is administratively burdensome and it will negatively impact marketing uses of data. A Deloitte study predicts GDPR could reduce expenditure in direct marketing by 34 percent or €18 billion and result in a €62 billion loss in sales from the European economy.

This further underscores the importance of data governance and data ethics as a means to build and retain trust in our industry. When businesses are accountable and data



governance is strong, consumer trust grows. Trust is an economic lubricant. Businesses that use data in ways that encourage trust, can then focus on using data to drive economic growth. The reverse is also true. When lapses in data governance result in a security breach or data use incident, consumer trust is eroded, and the risk of regulation that may harm business growth increases.

Unfortunately, the impact of a data governance failure on consumer trust goes beyond the company responsible for the lapse. Each failure has a cumulative effect on the psyche of consumers, regulators, and law makers, which increases the likelihood of restrictive regulation. To sustain a vibrant digital economy, all entities that collect, activate or use consumer data must be accountable and ethical. Trust cannot be an afterthought. We must work in partnership to ensure the right protections are in place.

HOW ACXIOM AND LIVERAMP MANAGE DATA GOVERNANCE

Acxiom was founded nearly 50 years ago, and has been a leader in data governance and ethical data use since its earliest days. We were the first company to hire a Chief Privacy Officer, the first to pioneer a Safe Haven data architecture for privacy-compliant data matching between businesses, and the first to launch a consumer portal (aboutthedata.com)

to increase transparency and understanding about how data is sourced and used.

Since the acquisition of LiveRamp, we have made numerous investments to ensure all operations meet our strict standards, including achieving SOC2 certification and operating LiveRamp within a certified Acxiom Safe Haven data environment.

> Today, we operate an "accountability based" data governance program, which means our executives are committed to ethical data use, and we have the operational means to put our commitment into practice.

Our governance program includes the following core elements:

1. **Formal Governance Program with Board Oversight** – we maintain a formal Enterprise Risk Management program with an independent risk leader that reports directly to our Executive Committee and Board of Directors. This organizational model provides an independent layer of oversight to ensure that the leaders of our security and privacy programs are accountable for implementing controls.

2. **Data Privacy Impact Assessments** – policies are meaningless if they aren't followed. We operationalize our policies for security and ethical data use by conducting Data Privacy Impact Assessments for the data sources that touch our systems, the workflows we support, and the code we write. We believe it's vital to perform this work at the design layer, not after the fact, ensuring that governance and ethics are built in rather than bolted on. In total, we conduct over 800 Data Privacy Impact Assessments each year.

3. **Privacy and Security Audits** – in addition to the formal third-party audits required for our compliance certifications, we perform our own internal audits, and we conduct approximately 50 audits of our policies and controls each year in partnership with our clients. As anyone who has participated in these audits can attest, we take a very conservative approach to data governance requirements, and we are firm believers in the importance of understanding vendor partner security practices.

4. **Risk Assessments** – the security and privacy landscape is constantly changing. To ensure the right level of data governance is in place, we go beyond efforts to ensure controls are in place. We also conduct internal and external risk assessments to determine what new controls need to be added to ensure data governance remains effective.

Our program continues to evolve in response to the innovation we see in our industry. More and more data in the world is observational, relating to human behaviors. For example, smart cars have hundreds of embedded sensors for everything from autonomous driving to measuring driver alertness. The principles of notice and choice that have guided our industry can be challenging to apply in many contexts. Advances in machine learning and artificial intelligence are also raising questions about how data-driven algorithms may shape cognition and culture in unintended ways.

To address these developments and more, Acxiom takes a proactive stance to mitigating risk by engaging annually with over 30 regulators and industry associations that set policy around the world. Through our engagement, we educate policy makers on the economic benefits of data use and guide policy

development toward outcomes that balance the needs of business and society as a whole in addition to protecting consumers. These interactions also give us a seat at the table to understand what regulatory changes are coming and when.

GETTING READY FOR GDPR

We already know that GDPR and the upcoming ePrivacy Regulation that governs digital data such as pixels, cookies, and mobile IDs use will vastly change the way businesses collect, manage, and use data. While the impacts will be greatest in Europe, the laws also apply to companies around the world that manage data on EU citizens. We are also seeing a "GDPR-ization" of data protection law in other countries, so it's even more important that business are thoughtful and deliberate in their operational readiness for GDPR.

Under GDPR there are new rules around the right to be forgotten, data portability will demand faster processes, and fines of up to 4% of annual global turnover or €20 Million (whichever is greater) for non-compliance will be possible. Identifying and demonstrating a legal basis to process data will be more challenging, including obtaining a valid consent or conducting a legitimate interest balancing test that the regulators agree with.

Brands will have to more actively demonstrate to regulators how protections, such as pseudononymization, are built into their operations. In a post-GDPR world, organizations will have to determine, among myriad other things, what permissions they currently have, which data they own, and how to track consent.

Although the final rules around GDPR are still being written, Acxiom has already taken proactive steps to ensure our operations will be compliant by the May deadline.

Because our global data protection and data governance program is built on ethics, we have always designed privacy and data protection into our products and services – a new requirement under GDPR.

We've also used GDPR-readiness as a catalyst to tune and improve our program. We have completed our data mapping exercise, and we are working with our clients and suppliers to ensure an optimal level of transparency is in place. We are happy to keep you informed as we complete our GDPR roadmap in the run up to May 2018.

In addition to taking steps to ensure our own operations are compliant, we have consulting offerings available to help our clients and partners with their own readiness efforts. These offerings include assistance with education on requirements, data mapping, transparency, and operationalizing data governance long term.

Our belief is that GDPR is best viewed as an opportunity to build or evolve an effective data governance program.

The smartest companies will leverage the focus it generates to create a competitive advantage that puts them in the best possible position to take advantage of new innovation coming online.

ACXIOM's 2017 Data Governance CHECKLIST

This is an important year in our industry for data governance. The stakes have never been higher. To help our clients and partners take an optimal approach to this important responsibility, we've created the following 'Top 10' checklist of key questions to ask and recommendations to consider:

1. **Do you have full leadership commitment to programs that ensure data governance including security and appropriate, legal, and ethical uses of data?** Executive support is critical, and this topic has increasingly become a board-level discussion.

2. **Do you have internal and external risk management programs for ongoing oversight and monitoring?** These programs can be vital for ensuring that data governance is effective and appropriately resourced.

3. **Do you have a current map of your data assets along with clear policies for data collection, integration, retention, and deletion?** Consider engaging an outside firm to help you audit what you have, identify remediation opportunities, and advise on policy updates.

4. **Do your current information practices align with your privacy policy? Do you have mechanisms to put your stated policies into place and evaluate your different data uses?** If you're not completely certain, perform an audit to identify gaps.

5. **If you receive data from a third party, are you clear on their privacy and security stance? Do your vendor partners undergo regular privacy and security audits?** Where uncertainty exists, consider engaging Acxiom to perform a Privacy Impact Assessment.

6. **What security and data protection requirements are bound into your contracts?** Ask your privacy and risk teams to conduct a review and tighten protections where necessary.

7. **Do you understand how the upcoming GDPR and ePrivacy regulations will impact your business? Do you have the right requirements in place to support opt-in permissions, right to be forgotten requests, and other needs?** Consider engaging Acxiom to help you put a roadmap in place.

8. **Do you have privacy engineers in house?** If not, consider hiring engineers with this expertise or engaging outside experts to train existing team members on how to operationalize data governance and ethics in your software code.

9. **Does your data governance plan include policies that can help you safely harness new innovations and data sources?** Implement an ethical framework that can make your program more future-ready.

10. **Do you face significant exposure to the risk of identity theft or fraud in your consumer authentication processes?** Consider exploring Acxiom's growing set of identity verification and authentication offerings.