The New Codes
of Conduct:

Guiding Principles for the Ethical Use of Data

By Jennifer Glasgow and
Sheila Colclasure

acxiom™

One
Introduction

Long before we were ever linked through The Social Network, we were all connected by an idea called

The Social Contract

One
Introduction

No need to brush up on your Hobbes, Locke and Rousseau.

The Social Contract theory made one simple observation: that we live in a world of "interconnected individuals" who are required to adhere to a set of rules mutually agreed upon by those individuals.

This is not a set-up for a history lesson on the Age of Enlightenment. However, this preface serves as a reminder that a discussion on what it means to live in a connected society is not new. Debates over the proper wielding of power and the definition of ethics are as ancient as civilization itself and are as relevant now as they have ever been, perhaps more.

Every day, we witness what happens when commonly accepted rules of ethics – written and unwritten – are not followed. Housing markets collapse, politicians fall from grace, and corporate reputations are tarnished. More often than not, these failures stem mainly from a lack of moral authority and actions taken without consideration of the vast implications of misconduct.

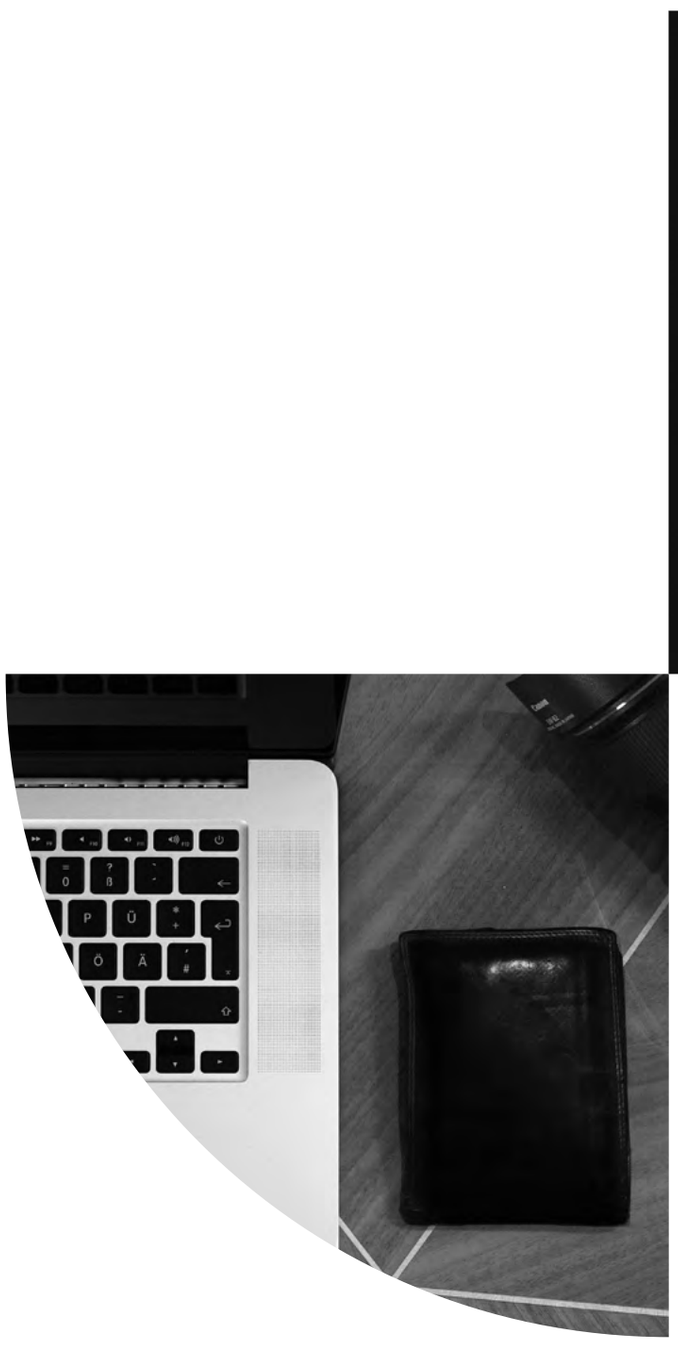
In today's information age, data holds the ultimate power. The public entrusts market players everywhere to use data with the goal of providing real value. And the individuals who work at organizations that house this data are expected to act collectively in accordance with agreed-upon cultural and social norms. Profit-driven or not, their underlying motives must reflect an aspiration to serve the common good, and to do no harm – whether that's by providing the public with a superior search engine, a smarter power grid or just more relevant movie recommendations.

Acxiom has been at the forefront of this discussion for more than 45 years. Today, almost half of the Fortune 100 companies trust us to manage their expansive marketing database operations, and we are regularly recognized as an industry leader in data privacy, data protection and security practices. Going beyond legal and regulatory guidelines, we work every day to manage, integrate and activate data based not only on what "can" be done in the market but also on what "should" be done, carefully considering what is appropriate and fair to all stakeholders, including the brand and the consumer.

This booklet, "The New Codes of Conduct: Guiding Principles for the Ethical Use of Data" shows how thinking and acting with data presents marketers with new and old challenges alike and how by deliberately applying an ethical construct to assess information-driven solutions, brands can leverage data to succeed in their respective marketplaces while establishing and strengthening the trust of the individuals they serve.

acxiom™

Two
Defining the Ethical Use of Data



Most consumers don't aspire to become experts in data-driven marketing. **What they want is a better experience and to be recognized as a valuable customer.**

Two
Defining the Ethical Use of Data

Today, more than any time in history, data and technology fuel our day-to-day lives. Educated consumers know brands use data to increase relevance and personalization. They provide their zip codes and request receipts via email. They sign up for loyalty cards for shopper rewards expecting the brand to "know" them, improve the product or service they provide and recognize their value as customers.

Frequently, however, most consumers either don't fully understand or care how data is collected and interpreted, what exactly is tracked or how that information will be used or shared – as long as they receive a better experience, are more quickly and accurately recognized and get the improved service they expect. In the past, those who provided such details had no choice but to implicitly trust their customer information would be treated with care, as part of the brand's promise to them. Today, such trust is not so easily given.

In the marketing and advertising arena, we are starting to see some tension in this arrangement. Consumers are asking brands to place as high a value on their time as they do and expect any engagement between them to be contextual, relevant and valuable. More than ever, they can punish brands that don't clearly demonstrate they know how to treat personal data in a way that meets their expectations and can opt out entirely with ad-blocking technologies.

Even people who work in the advertising business or in a related marketing or sales field may not be aware of the extent of potential pitfalls they face when handling data. For marketers who grew up in the "digital first" era, this is especially true. As the anonymous cookie-based world continues to converge with real-world consumer data, ever-evolving analytics capabilities let these marketers learn a tremendous amount about consumers and potentially more than the consumer ever intended to reveal.

This is why defining the ethical use of data is so critical. Consumers expect companies to act ethically with their data to provide more relevant and contextual value that strengthens consumer trust and deepens loyalty. But they also feel it's not their job to sort it out – it's the responsibility of the companies that collect or have access to personal information to ensure the promises that come with the data are kept throughout the entire marketing process.

As in any relationship, business or otherwise, trust needs to be earned, sustained and nurtured over time. To succeed in the long run brands have to first be accountable. Therefore, a common understanding of what it means to act ethically with consumer data is required.

Without a common set of rules or proper governance, it's unrealistic to assume brands across a vast marketplace can meet this expectation and maintain the trust of the consumers they serve over time.

Two
Defining the Ethical Use of Data

So, you may ask, what about the role of government? If most consumers don't particularly want to fully understand how data is collected and interpreted, the regulators and enforcement authorities certainly do, and they actively investigate potential misuse. Surely legislators can create laws that help establish trust and regulate consumer protection. Can't consumers rely on them to enforce rules related to data collection and usage?

It's true that over the years, state and local governments have established stringent rules about practices involving telemarketing, commercial email and children's privacy. The Federal Trade Commission (FTC) protects America's consumers by preventing unfair and deceptive trade practices and taking action against entities with inadequate data security measures and inadequately disclosed information collection, use and disclosure practices. State attorneys general also typically have similar authority and take action, particularly in the case of high-profile data breaches. And regulators, particularly those in healthcare and financial services, have authority to enforce privacy regulations.

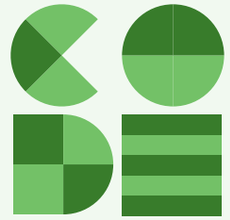
But many admit that when regulation finally goes into effect, whether state or federal, it can sometimes already be outdated. Today's business environment is innovating well ahead of the law. Just consider the recent explosion of technological advances such as internet-enabled vehicles, wearables, digestables, facial recognition and the digital home. All of these advancements have given rise to new data sources, which are often highly personal and contextual. Any attempt to slow down the pace of innovation would be futile and self-destructive economically. So inevitably, accountability for ethical practices must also be required at the organizational level, within the industry itself.

Even with governmental and regulatory bodies focused on the issue, it is commonly acknowledged that the speed of technological innovation vastly outpaces the speed of regulation.

The ethical use of data requires vigilant self-regulation, ongoing discussion and intense awareness of the potential implications for any misuse. If consumers detect some type of misconduct, companies may be sacrificing valuable trust, affinity and loyalty. And of course, profit. Claiming ignorance is never an option, and brands realize that in today's age of the empowered customer, there is huge risk if an ethical code isn't applied but also huge potential upside if they show the consumer respect through valued and welcome use of their data.

This may help explain why so many ethics courses and corporate training programs on consumer privacy are now mandatory – they're an attempt to ensure our future corporate leaders clearly understand the responsibility of power and that a high degree of trust between consumers and brands is required to succeed, grow and sustain the business financially and reputationally. It's simply good business.

Let's look back at what happened when there was no ethical structure, and the aggressive use of consumer information went unchecked.



Often the phrases "ethical code," "moral code," "code of conduct" and "code of practice" are used interchangeably, but there are some distinctions.

An **ethical or moral code** defines the underlying values for the code and describes an organization's obligations to its stakeholders. It is addressed to the public. It explains the organization's activities and the way it does business. It includes specifics on how the company plans to implement its values and vision, as well as guidance on ethical standards and how to achieve them. Ethical codes may also apply to the culture, education and religion of a whole society.

A **code of conduct** is generally intended for employees or members. It usually sets restrictions on behavior and is more compliance- or rules-focused than value- or principle-focused. Companies often adopt codes of conduct not to promote a particular moral theory but rather because they are seen as important for effectively operating an organization in a complex environment where moral concepts are critical.

A **code of practice** is a code of conduct a profession or organization adopts to regulate that profession or its membership. It addresses difficult issues and clearly defines what behavior is considered "ethical." Failure to comply with a code of practice can result in members being expelled from the professional organization.

Three
Do-Not-Call

Three
Do-Not-Call

In the U.S. and around the world, consumer data has been shared for marketing purposes for decades, especially in the catalog and publishing industries. As phone technology advanced in the late 1970s, outbound telemarketing gained prominence. Initially, the public considered telemarketing a worthwhile practice, and telemarketing quickly proved to be a highly effective way to reach consumers. Subsequently, it became a wildly successful revenue generator for brands and telecommunication companies.

However, over time, sentiment changed. Aggressive telemarketers, with calls often made at inconvenient times and with little consideration of preference, caused a consumer revolt against the intrusion of these calls. By the late 1980s, state legislatures began passing "Do Not Call" (DNC) legislation, eventually leading to the establishment of the Federal Trade Commission's Do Not Call Registry in 2003. In just 17 years, telemarketing went from one of the most lucrative marketing practices to being considered one of the most reviled and aggravating forms of communication.

Contrary to the norm, federal legislation was quickly passed. It was a huge win for policy makers and consumers who wanted to demonstrate that they would not tolerate the unsanctioned use of their data. This backlash nearly killed the telemarketing industry, and it changed the perception and effectiveness of the telephone as a marketing channel.

The advent of the DNC registry is considered a seminal milestone in the evolution of consumer privacy. Brands recognized that consumer tolerance is finite and must be conserved.

With more than 217 million consumers now on the do-not-call registry, this event humbled the industry and taught a basic lesson in customer relationship management. When someone asks you to quit contacting them, companies need to respect that request – even if no one is forcing them to. If this approach had been implemented quickly and properly, consumers may not have been pre-conditioned to reject a phone call, and receptivity to telemarketing might be thriving today.

The DNC registries that swept the nation became a turning point in consumer protection. It sent a signal to companies and legislators that they had to be more sensitive to what consumers cared about. Responsible companies began taking a hard look at their policies and evaluating how consumer perspectives should be considered in all their marketing communications. Companies began asking themselves, "Does this behavior constitute an ethical use of the data? Is it fair and respectful to the consumer? Do consumers feel like they have some amount of control? Does it consider their preferences?"

There are several ways to think about ethics, often viewed through one of the following lenses. To achieve the best outcome, it is important to employ a combination of all three:

1. Is it fair? Virtue-based ethics emphasize the importance of character and good habits in driving moral behavior. This is where the idea of "fairness" comes into play.

2. Does it infringe on individual rights? Duty-based ethics focus on obligation as the basis for ethical behavior. One branch of this field is the "rights theory," which considers rights as natural (not invented by man), universal (not cultural or country-specific), equal (for everyone regardless of gender, race, age, etc.), and inalienable (they cannot be sold, bartered or renounced). As an example, Europeans generally believe data protection is a fundamental human right.

3. Does it benefit the greater good? Outcomes-based ethics determine the rightness or wrongness of an action based on a cost/benefit analysis of an action's consequences. An action may be regarded as morally right if the consequences are more favorable than unfavorable or if it promotes the greatest utility for the greatest number.

Four
A Culture of Respect

The simple rule is:
When brands collect, integrate and apply data, they should always maintain privacy and respect the wishes of the consumer.

Four
A Culture of Respect

Do-Not-Call raised awareness of the importance of recognizing and honoring consumers' attitudes, concerns and preferences. Developing a culture of consumer respect is a fundamental requirement for brands, requiring them to consciously evaluate the data they are collecting and how they plan to use that data.

Today, though U.S. privacy laws and self-regulatory principles vary widely, companies that collect data are required to publish privacy policies (a disclosure of regulated personal information is also typical) that generally offer a pre-collection notice and an opt-out for marketing use of that information. These policies provide brands the consent needed to actively or passively collect consumer information.

Here's where it gets complicated. We used to live in a world of mostly active collection – when consumers were directly asked for information, like their name and address on a registration form. We now live in a world where 90 percent of data has been created in the last two years. With this explosion of data, we are moving more into an era of primarily passive collection, where consumer data is mostly observational or analytically created, requiring no explicit actions on their part – like cookies working behind the scenes on a web browser or a response score constructed from reviewing other data.

Now, even in a mostly observational world, brands still face material consequences for violating company policies or notices. Companies that infringe on the use stated in their disclosures are still open to prosecution by the FTC, state attorneys general and class action lawsuits. Having a balanced view of respect and the ethical use of data is a way for business leaders to mitigate brand risk and also potentially heavy fines imposed by regulators, sometimes totaling hundreds of millions of dollars.

Taking it a step further, defining a clear value exchange for the consumer – one that explains the value created from data in addition to the product or service – will help reduce consumers hesitation around sharing information. In adopting this approach, brands give consumers the better experience and service they expect, tangible value in exchange for data, and also an appreciation and understanding of why their participation is so important.

Defining a Value Exchange. Econsultancy's "Marketer's Guide to the Internet of Things (IoT)" provides an outline of three elements essential to demonstrating value. These elements must be present for consumers to engage with a brand over the longer term and move beyond data security and financial incentives:

Utility is a vital measure for any solution. Is the proposed solution actually solving a problem consumers have? The IoT will make us part of the network of interconnected objects and people. This will enable benefits such as "persistent identity," where we are recognized and doors unlock, travel is paid for and coffee is brewed.

Entertainment is another compelling reason why people use technology. It can push any technology through the resistance that inevitably comes when people consider new technologies.

Participation is a key driver of us all. We want to be part of the herd. The IoT connects us to a wider world of people and objects, creating closer links than ever.

Five
To the Power of the 1st

There's one defining market characteristic that necessitates the collection of data – competition.

acxiom

Five
To the Power of the 1st

U.S. consumers have an incredible number of options. Just think of all the products available today on Amazon. Everything from A to Z, in fact. With the proliferation of options, it has become harder for brands to understand exactly what consumers want or need or predict their choices. This makes the marketer's most basic dilemma even more difficult: if it's not possible to market to everyone, how do we efficiently reach those who are most likely to be interested in what we have to sell?

Increasingly, intense market pressures push brands to collect more and more data, all in an attempt to win new customers, keep existing ones and strengthen competitive advantage.

Today the war for attention has intensified, heightening the pressure to find new customers and keep existing ones. So to find the most receptive audience for their products or services, marketers collect data through a variety of methods. In return for signing up for loyalty cards or enabling cookies, consumers receive more contextual and relevant offers, conveniences based on preferences or tailored rewards – all resulting in a better brand experience that hopefully drives future engagement.

To quickly review, first-party data is collected and owned by the brand and often includes personally identifiable information (PII) like name, address, age, and marital status. First-party PII is considered the most valuable data a company can have and becomes the core of any marketing database. It's this "known" information, these identifying elements, that become a critical foundation for all data-driven marketing activities. But this data also comes with rules that are now forever tied to the data. Case in point: if the intent to share data was not initially disclosed to the consumer at the point of collection, brands should not provide it to a third party. Furthermore, responsible marketers should be accountable for awareness and compliance with the rules associated with the data they collect, create and use.

But interestingly, first-party data can also be anonymous, collected without specific identity markers and often with fewer restrictions on terms of use. For example, cookie-based on-site behavior analytics and social interactions are also considered first-party data, including information stored in data management platforms (DMPs) and tag management systems. This data is especially valuable in helping a brand understand which content and offers on its website are pulling people in, driving more time spent on their site and bringing them back but it's often not tied back to an individual.

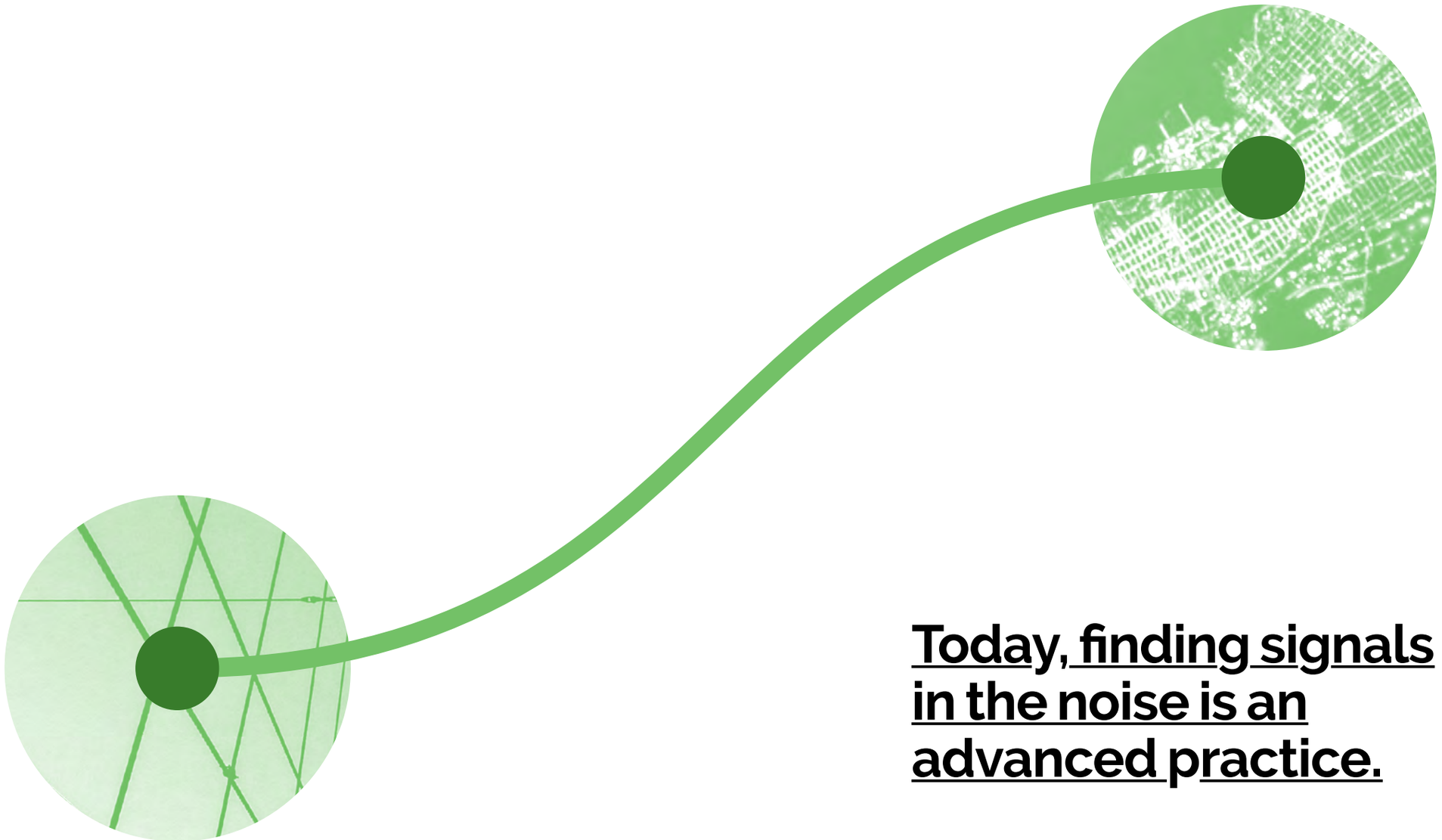
Marketers also enrich customer records with each engagement, purchase and stated preferences to optimize offers. With all the different types of first-party data, both known and anonymous, marketing analytics teams can develop derived or modeled insights based on sophisticated analytics to infer things about a consumer – such as whether or not they are in-market for an SUV or enjoy cooking. To attract and convert prospects, they leverage the valuable segments created on existing customers to produce "lookalike" models to help them find consumers likely to be in-market for the same products and services.

But let's consider what happens when a marketer seeks more prospects and runs audience propensities based only on first-party data, which then drives all of next quarter's media plans. What if the marketer knew half of the "most loyal" customers, the ones the model was built on, are actually spending twice as much with a competitor? Marketers are discovering that the combination of first-party data and derived insights will only take a data-driven marketer so far. While many brands have invested heavily in building the infrastructure and analytics capabilities to enable true data-driven marketing, they have discovered that these insight-based campaigns are only effective if they're starting with all the relevant and accurate data available, which includes first-party data but more often also includes second- and third-party sources as well, all part of a growing data marketplace and discussed further in Chapter 8.

Applying ethical consideration to the collection and use of first-party data spans the complete lifecycle of CRM data management including:

- Data origination
- Permissible uses of collected data
- Access to the data
- Controls around the data
- Methods of distribution
- Use cases enabled
- The process for updating, refreshing or replacing
- Data removal and deletion

Six
Analytics Advances



Today, finding signals in the noise is an advanced practice.

Six
Analytics Advances

For decades, marketing analysts have drawn simple inferences from the data they have to better identify and understand their best audiences.

Let's say an individual subscribes to a hunting magazine. If he also owns a hunting license, marketers assume he has an interest in hunting. If a consumer frequents travel websites and makes travel-related purchases, marketers conclude she, or a family member, likes to travel. These common-sense approaches have been pretty accurate in identifying what a person shops for and consequently might want to buy. Overall, they worked well for marketing purposes and were certainly much better than having no data at all.

For example, marketers can determine consumers' propensity to travel abroad, or if they have characteristics in common with those who enjoy fine wine. These analytical approaches all result in predictions that are usually, but not always, accurate. These predictions are often effective enough – again, better than having no data – for identifying audiences for advertising and marketing purposes.

In today's online world, the process of matching data is also advancing rapidly. More and more, marketers are using deterministic matching when combining data sets, which uses PII data. Once a match is established, this means both targeting and measurement can take place at the individual level instead of the device level, and gives marketers both the reach and the accuracy they need to sequence messaging, cap frequency and suppress targeting. For example, if you've realized you've seen the same display ad over and over, chances are you don't need to see it again. Or if you've already bought the item, you don't need a reminder that you were interested in it.

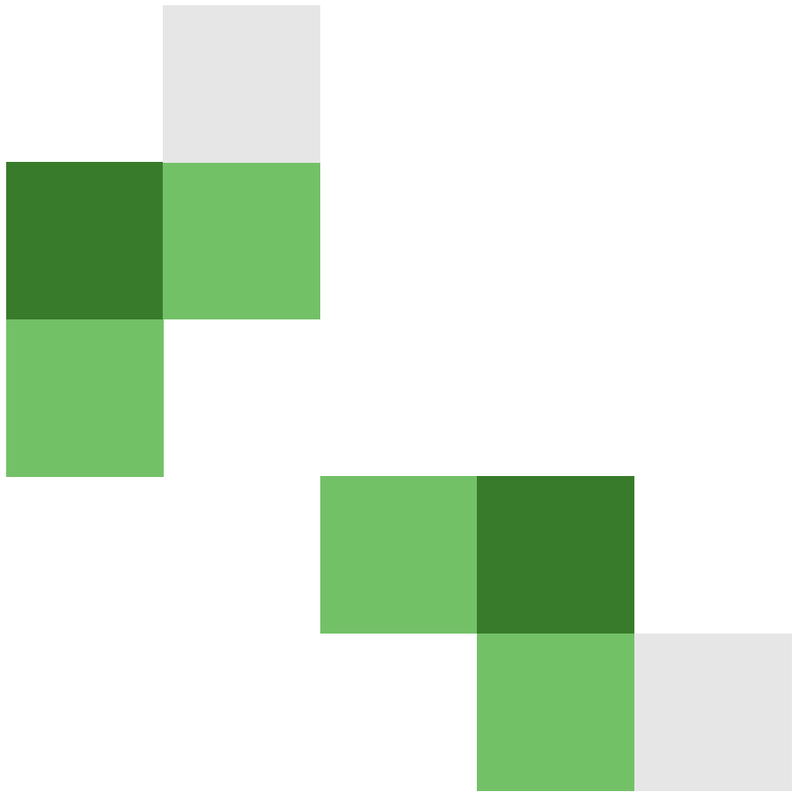
With the need for accurate deterministic matching and sophisticated analysis of larger and larger data sets, it's becoming more important for marketers to use partners to de-identify and match data in a privacy-compliant way. This gives brands the freedom to provide individuals with more customized and seamless interactions and evolve their algorithms through post-campaign analysis without compromising any personal information. By adopting this kind of people-based marketing, brands can close the loop on their campaigns, understand attribution and return on marketing investment, but most importantly they never stop learning how to provide a better experience for their customers.

Six
Analytics Advances

If deterministic matching is not available or not feasible at the scale required, marketers can revert to probabilistic matching to estimate, for example, the likelihood that two devices relate to the same individual – although this approach generally favors reach over accuracy.

Historically, data matching and the subsequent creation of new insights through analytics are calculated periodically and stored in a file. Today they are more often calculated on-the-fly based on the most recent data available, and new insights can be generated minutes or even seconds before they are used in real time or near-real time. Such predictions are not only made by companies planning to use them themselves; third parties often make analytical predictions and sell them in the marketplace. In other words, a social media site or a marketing data partner may predict that a consumer is in the market for a new SUV and sell that prediction to auto dealers.

The proliferation of analytics and the number of companies that use them have grown exponentially in just the last few years. Sophisticated analytics have led to superior data, which has powered innovation and significantly enhanced results. And while the marketing industry understands many of the extraordinary benefits big data analytics offer, consumers often feel that the use of data may be crossing the line to intrusive, unwelcomed and potentially nefarious use. Today's analytics have expanded far beyond simple inferences. Modern marketers have the ability to use data to accurately predict things that were previously unimaginable and even potentially unethical.



From an analytics perspective, there are several types of statistical approaches marketers have learned to leverage:

1. **Simple Derivation:** a subscription to Golf Digest equates to an interest in golf (widely used in the 1970s–1980s)

2. **Statistical Model:** people with a certain size house in a certain zip code who subscribe to financial magazines and have a graduate degree are likely to have an income within a certain range (popular in the late 1980s)

3. **Population Segmentation:** people of a certain age who live in certain neighborhoods and drive certain types of cars are likely to fall into a certain demographic group, e.g., baby boomers (popular in the early 1990s)

4. **Propensity Score (sometimes known as a lookalike score):** a group of people who have predominant characteristics (certain age, certain income, certain education, certain hobbies) can then be overlaid on another population of people to find more individuals or households with the same characteristics; for example, people who often travel abroad exhibit certain demographic characteristics, and others with those same characteristics are also highly likely to be interested in traveling abroad (popular in mid-2000s)

acxiom

Seven
The Practice of Handling Sensitive Data

Seven
The Practice of Handling Sensitive Data

Now that we've reviewed some analytical techniques, let's consider some "real-world" scenarios that demonstrate the implications of new technologies and how they are allowing marketers to collect more data and also do more with it.

First, a consumer downloads a popular gaming app, and allows it to use his or her location, essential to playing the game. In this particular case the consumer is made directly aware of the tracking, but he or she likely doesn't realize the full extent of the information the app captures and all the potential uses or applications. Fitness trackers, another popular trend, are collecting vast amounts of potentially sensitive data on sleep habits, diet and fitness. What potential uses, or misuses, can result through even the most cursory analysis of this data? What unintended consequences may result?

With the dawn of the Internet of Things, we are entering an era where objects – appliances, cars, wearables, ingestibles and more – are collecting data on consumers, and the risk of joining together data to create a customer view that is now deemed sensitive is only increasing. The responsibility of how that information is collected, shared and applied will become increasingly complex and requires a rigorous set of policies and processes for ethical and acceptable uses. Brands must be able to understand where the "line" is and understand that line will move over time.

Let's say a consumer recently purchased an internet-enabled vehicle, which can collect data ranging from location, speed, time and even the driver's level of alertness. And let's say the manufacturer is allowed to share this data with other third parties, like an insurance provider. What happens if that provider looks to increase your premium after reviewing your alertness history or whether you happen to drive more at peak traffic times or through bad weather? Could the company charge you more for driving faster than your neighbor? Or on the positive side, perhaps your premium could go down if you drive slower or drive more during off-peak hours. Could more advanced fitness trackers tell if you're having a heart attack? Should it be able to call 911? These are complicated questions, and the potential risks and benefits to the individual and society will continue to prompt vigorous debate and discussion.

"Our collective challenge is to make sure that big data analytics continue to provide benefits and opportunities to consumers while adhering to core consumer protection values and principles."

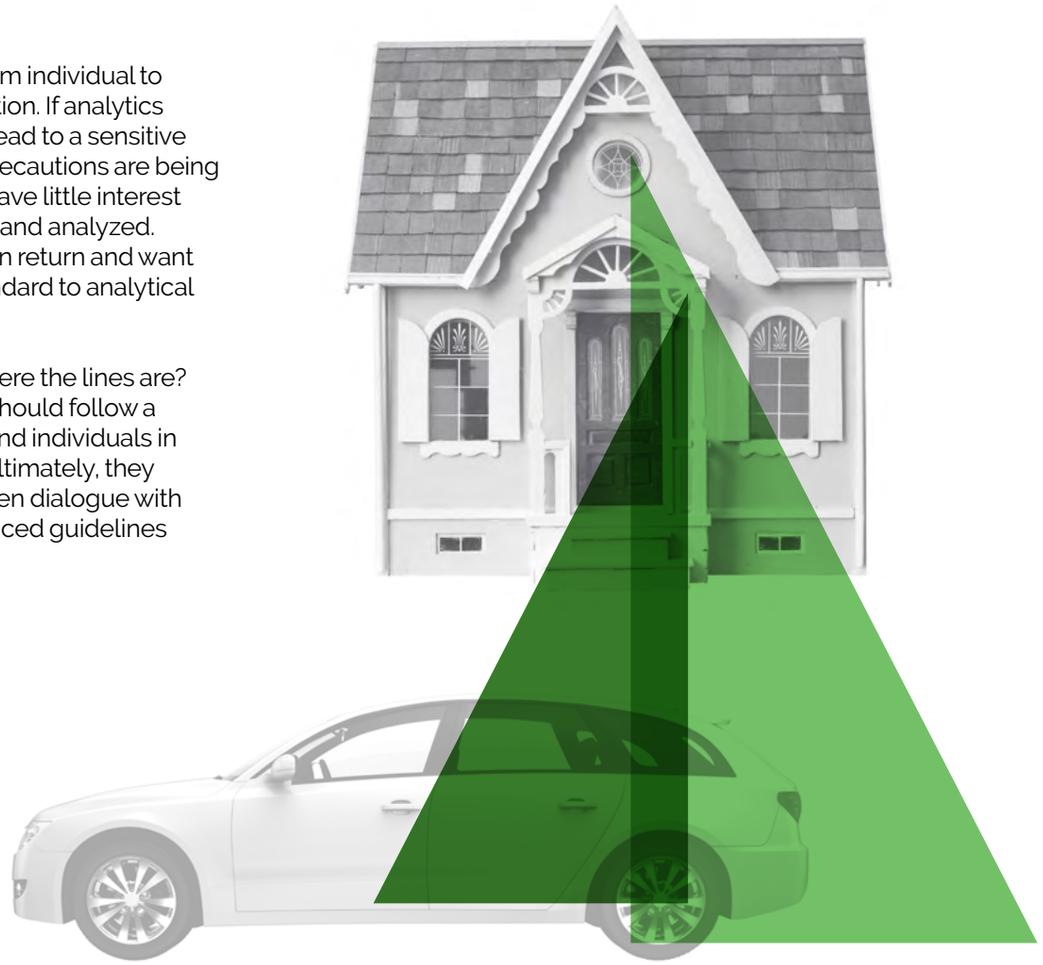
The Federal Trade Commission

Seven
The Practice of Handling Sensitive Data

In January 2016, the FTC published a report titled: Big Data: A Tool for Inclusion or Exclusion? In it, the commission addresses concerns with the commercial use of consumer information, focusing on the impact of big data on low-income and underserved populations. While the FTC acknowledges that big data analytics has the potential to offer many positive societal benefits, it's illegal to use data to exclude parts of the population for eligibility purposes. For example, if big data analytics shows a lender that single people are less likely to repay loans than people who are married, a lender cannot refuse to provide a loan to a single person or offer less favorable terms. This would be deemed discriminatory behavior.

Consumer concerns about big data vary widely from individual to individual and perhaps even generation to generation. If analytics of non-sensitive data can create sensitive data or lead to a sensitive use of data, the question arises: do I trust proper precautions are being taken? As we discussed earlier, most consumers have little interest in knowing the details about how data is collected and analyzed. They simply care about the value they are getting in return and want to feel confident a brand is applying an ethical standard to analytical processes so lines aren't crossed.

So how exactly do brands and regulators know where the lines are? It all goes back to the social contract. Companies should follow a set of rules mutually agreed upon by businesses and individuals in their society. A consumer "knows it when I see it." Ultimately, they are the ones drawing the lines. Only through an open dialogue with consumers can those who use data develop balanced guidelines that maintain consumer trust.

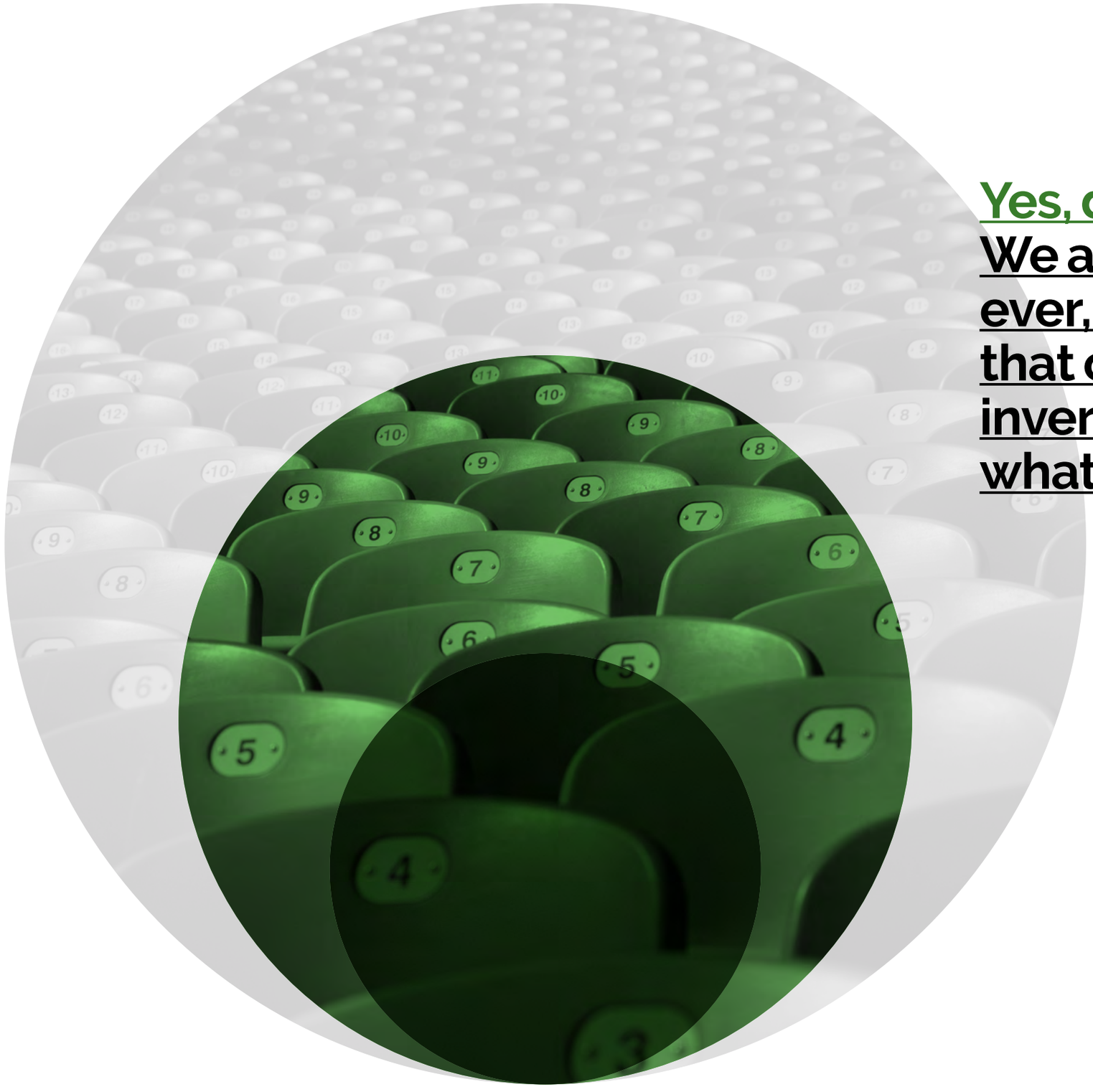


Degrees of Sensitivity
The Direct Marketing Association (DMA), Digital Analytics Association (DAA) and Network Advertising Initiative (NAI) define sensitive data as described here. Each code of conduct has certain restrictions or prohibitions on the use of sensitive data.

- Third-party behavioral and multi-site data used for interest-based advertising that is collected from children younger than 13 on child-directed websites must be collected in compliance with the FTC's Children's Online Privacy Protection Act (COPPA) and can only be used with parental consent.
- Third-party, multi-site data containing financial account numbers, Social Security numbers, pharmaceutical prescriptions or medical records about an individual cannot be used for interest-based advertising without opt-in consent unless the records are de-identified according to HIPAA regulations.
- Behavioral or multi-site data used for interest-based advertising is prohibited from being used for eligibility determination for employment, credit standing, healthcare treatment and insurance underwriting.

acxiom

Eight
A Growing Data Marketplace



Yes, data growth is exponential. We are more connected than ever, but it's the enterprises that collect the data that are inversely responsible for keeping what we create protected.

Eight
A Growing Data Marketplace

As the number of data sources continues to grow – one exabyte at a time – and more data is collected, shared and sold between different parties, adequately defined data governance becomes even more essential for brands to safeguard consumer privacy and prevent a breach of trust.

Brands may have built strong capabilities for properly leveraging their own data for marketing purposes, but with so much other data available, marketers are now looking outside for ways to supplement their understanding of their customer – for example, to help drive stronger brand affinity and share of wallet. While first party is king, it can only provide a limited view of customers, because most of what people do or what they buy every day is outside of a single brand's line of sight. To enhance their view of the customer, for example, wouldn't it help if companies knew where else customers and prospects shop and what kinds of products they buy (perhaps finding out that their most loyal customers are actually spending a lot more with a competitor)? Having this knowledge could completely change a brand's whole segmentation and targeting approach, giving media teams an entirely new direction for planning.

Luckily, marketers have plenty of choices. Second-party data – data shared between partners for mutual benefit – can potentially provide a steady stream of appended data that enhances their view over time and help them engage customers in a more contextual and personalized way. For example, in order to deliver more targeted offers, airlines can partner with travel and leisure brands to pinpoint consumers planning trips. But building relationships with partners or providers of data that have valuable data sets takes time and resources. Marketers can also consider a variety of third-party data sources, usually aggregated data that can be bought, such as from a marketing data provider. Survey or modeled data are common examples, and they can quickly tell a brand more about customers' interests or if they fall into a specific psychographic or demographic segment.

"More than 70 percent of the digital universe is generated by individuals. But enterprises have responsibility for the storage, protection and management of 80 percent of it."

IDC

Eight
A Growing Data Marketplace

As marketers extend their use of data beyond the boundaries of their brand, there is much to consider when choosing the right partners, data providers and publishers to buy from, including how to validate both the accuracy and provenance of that data. With so much data available – structured and unstructured, PII and anonymous – the decision of what to source and from whom can be paralyzing. A thorough ethical interrogation is required to ensure proper data governance policies and processes were in place when the data was collected. What is the source or origin of the data? What was the consumer expectation when the data was collected? Were consumers provided proper notice and choice? Will the joining of this data cross a line that may be undefined but is apparent if you know your customers? Are we able to integrate these new data sources with our own data in a privacy-compliant manner?

Marketers should already know that when data is collected it is imbued with certain rules that become attached to the data for the life of that data. They need to become more aware that they are held accountable for how they collect and use their own first-party data, and when they work with outside parties they now become "their vendors' keeper" as well. More data integration raises a series of new and complicated set of responsibilities for marketers and significant considerations for brands as they weigh the risks and rewards of buying and selling data. The risks must be identified at the outset to determine what data can be shared to ensure that each use case is acceptable to consumers, whether explicitly stated or implied. This is often a mix of regulatory compliance as well as acumen and empathy.

When looking to integrate multiple data sources, it's a good practice for marketers to consider anonymizing the data first. Brands more often are sharing the burden, working with a neutral third-party partner offering policies, processes and an ethical code for ensuring consumer data privacy protections are safeguarded. As the data economy evolves and more brands start to monetize their own data to build new revenue streams, the sustainability of the data marketplace depends on such responsible practices.

The U.S. Direct Marketing Association (DMA) has developed guidelines for companies sharing their customer data to give notice to consumers and offer them the ability to opt out of sharing, and these guidelines provide more information on appropriately sharing data for marketing purposes. Over the years, other ethical standards addressing such issues as list rental agreements and data compiler practices have been incorporated into the DMA's guidelines for ethical business practices.

acxiom

Nine
Complications of a Global Economy

Brands that work internationally have the added complication of rules and regulations concerning data moving across borders.

acxiom

Nine
Complications of a Global Economy

Approaches to consumer data privacy and protection vary widely across the globe and can range from "highly restricted" use to "effectively unrestricted" use. In the United States, regulations on the collection, use and storing of personal data would be categorized as restricted. However, the European Union's approach to consumer data privacy and protection is even more restrictive.

Across Europe, historically where privacy is considered a fundamental human right, the right to privacy is a highly developed area of law. In Europe, privacy extends to any data that can relate back to a single person and informs the regulations that provide the rules across the EU for permissible use of personal data for marketing purposes, as well as many other applications, such as offering credit.

One of the most high-profile examples of geographical differences in data regulation comes from the European General Data Protection Regulation (GDPR), which will take effect in 2018, replacing the Data Protection Directive established in 1995. GDPR will become the law of the continent regarding collection, use and application of personal data, and according to its charter, this statute will provide EU citizens more control of their personal data and simplify the regulatory environment for international business by unifying the regulation across the EU.

Let's take a look at what GDPR will regulate and its impact on marketers and the marketing and ad tech ecosystem:

Harmonization:

Replacing the patchwork quilt of EU member state laws that make up the current Data Protection Directive, the GDPR will, for the most part, be universally applied throughout the EU. For most companies operating in different EU countries, the lead Data Protection Authority (DPA) of the country where that company's headquarters is based will have the oversight and the power of enforcement for operations Europe-wide. This means a company operating in multiple European countries can focus on its lead DPA's guidance when it is issued.

Enhanced privacy notices:

The GDPR regulation requires more detailed privacy notices, including information on the reason why (including legitimate interest) companies want to use personal data in a certain way, as well as contact details of the data protection officer/privacy officer.

Consent:

GDPR requires "unambiguous" rather than "explicit" consent, which is interpreted as a stricter definition. While further guidance from the regulator is expected, it is anticipated that carefully crafted, implied consent mechanisms could meet the standard of unambiguous consent. Separately, collecting data from minors younger than 16 will require parental consent. This age limit may be lowered by the different EU member states.

Right to object to segmentation:

Consumers have the right not to be subject to the result of automated decision-making, including profiling. When delivering personalized advertisements, generic segments such as affinity scores or tailor-made customer groups are often used. In marketing terms, profiling refers to systems for consumer segmentation. Companies must ensure a robust opt-out mechanism is in place to ensure personalized advertisements are not shown and/or delivered to consumers who object to being assigned to a particular marketing segment.

Non-profit organizations act on behalf of consumers:

The GDPR formally introduces the U.S. concept of class action.

Maximum Fine:

Companies found to be in breach of GDPR can be fined as much as 20 million Euros or 4 percent of their worldwide annual revenue – whichever is more.

Data Protection Officer:

GDPR may require companies collecting consumer data to appoint a data protection officer (DPO). GDPR grants consumers the right to contact the DPO on all issues related to their data.

Right to erasure:

A so-called right to be forgotten was replaced by a more limited right to erasure.

Nine
Complications of a Global Economy

Along with the GDPR, the Privacy Shield negotiated between the U.S. and the EU will also regulate transatlantic data flows and replace the European Commission's 2000 Safe Harbor Program. Safe Harbor was invalidated in October 2015 following the European Court of Justice's ruling after a user complaint regarding insufficient protection of Facebook data.

So what does all this mean for companies doing business around the globe, and in particular, multinationals operating in the EU? Based on the requirements and provisions, it appears to reflect a healthy compromise between privacy and business use. The EU's updated personal data protection requirements extend the scope of the EU data protection law to all foreign companies processing EU residents' data. As outlined, GDPR harmonizes the data protection regulations throughout the EU, making it easier for non-European companies to comply. But this extended scope that allows more effective compliance across borders comes at the cost of class action litigation and potentially very severe penalties of up to 4 percent of global annual revenue.

It's clear Europeans have a markedly different philosophy when it comes to protecting personal data. That philosophy is grounded in privacy being a human right, akin to our first amendment. The importance of the U.S. safeguards currently in place will only increase with the expansion of our personal data footprints and as our culture as a whole thinks about the appropriate uses of data.

In other countries and on other continents, the trend is generally moving toward more stringent regulations for how personal data is collected, used and applied. This will put greater pressure on the marketing industry, whose business relies heavily on this data. Brands that own first-party data and also use second- and third-party data must ensure they have rigorous policies and safeguards in place, from both a global regulatory and brand perspective.

The trend lines are clear – the increasing globalization of our economy and commerce will increase the need for agreed upon approaches to assure ethical use when collecting, integrating, applying and transferring personal data from around the globe for marketing purposes. Marketers continue to innovate well ahead of the law and accepted industry code of conduct, and we must extend that innovation to our approach to privacy-compliant policies and processes that protect and provide value to consumers, brands and the marketing and ad tech ecosystem.

There are also numerous advertising codes in the U.S. and internationally, including the New Zealand Advertising Standards Authority Code of Practice, the UK Advertising Code of Conduct, the Advertising Standards Authority of South Africa and the FEDMA Code of Conduct in Europe.

Ten
Defined Guidelines for Ethical Use of Data

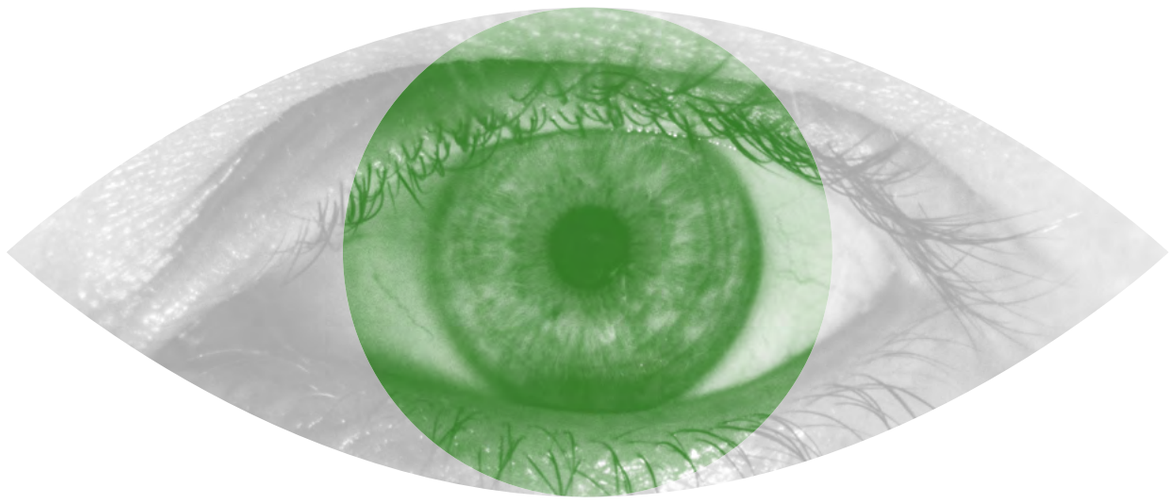
As an industry, we must classify behaviors and provide definitions on what constitutes the ethical use of data.
The time to advocate for these recommendations is now.

Ten
Defined Guidelines for Ethical Use of Data

Going back to a philosophical definition, ethics seeks to resolve questions of human morality that involve systematizing, defending and recommending concepts of right and wrong conduct. As marketers, we also need to adhere to a sense of what is right and what is wrong.

Ethics evaluates what actions are right or wrong in particular circumstances. Brands needs to operate under evolving standards and codes that ensure consumers are protected and, in fact, they have been guided by codes of conduct for many years. At a high level, worldwide advertisers must comply with the law in each geography. They should also be truthful, not mislead or deceive and be socially responsible. But it's also clear that gaps in guidance now have emerged, such as:

- New examples of sharing data for marketing and advertising purposes (both PII and anonymous information)
- Appropriately employing sensitive data for marketing and advertising purposes
- Ethically applying robust analytics (e.g., big data analytics) for marketing and advertising purposes



Ten
Defined Guidelines for Ethical Use of Data

In September 2014, Acxiom Corporation hosted a unique forum at the National Press Club in Washington, D.C., to address the ethical challenges of big data in today's data-driven marketing ecosystem. It was the first gathering of its kind to promote an in-depth discussion of these important issues. The select group of 30 invited participants included government regulators, academics, industry trade association executives, legal experts, think tank officials, consumer privacy advocates and business leaders. During the daylong series of meetings, discussions and presentations, the group identified five areas where stronger ethical principles should be introduced and developed broad recommendations for:

1. **Maximizing transparency and choice.**

   Posted privacy policies must be clearer about the use and sharing of consumer data for marketing purposes.

2. **Classifying data and mitigating use risks.**

   Marketing data should be classified to identify various types of risks, and appropriate mitigations for these risks should be put in place. Marketing data should be anonymized whenever possible.

3. **Limiting downstream risks.**

   Data is often shared several times by intermediaries before it reaches the ultimate user, the marketer. Marketing data providers should have contracts with all downstream users of the data to ensure it is always used appropriately, prohibiting discriminatory marketing practices and the use of marketing data for eligibility purposes (e.g., credit, insurance, employment).

4. **Helping enforce ethical practices.**

   Everyone in the marketing community should help the appropriate authority – whether a self-regulatory entity or a regulator – enforce ethical practices by reporting bad actors to the appropriate enforcement body. A defined process for investigating and taking appropriate action should be in place for the whole ecosystem.

5. **Educating consumers about common marketing practices.**

   The marketing industry should support and engage in developing education for consumers about common marketing practices so consumers can exercise the choices they're offered in an intelligent way – not just because they are afraid of the unknown. One example of this type of education is the Council of Better Business Bureaus' Digital IQ project.

Eleven
Understanding Risk

Eleven
Understanding Risk

What happens when clear ethical guidelines aren't in place? More and more, when consumers think their personal data has been collected and used in ways they don't like, they will make their voices heard. Consumers are speaking out about their negative experiences, empowered by social media along with traditional word of mouth. Social media not only strengthens the consumers' voice, but also allows them to galvanize others to express discontent, and effectively campaign against brands.

Consumers' unease can affect a brand directly and also the advertising industry as a whole. This recently has taken the form of ad blockers, ad choices opt-out, and most recently app choices opt-out – all clear examples of backlash against all advertising, not just specific brands (and also against the high cost of downloading data). The issue of collection, use and application of data – both known and anonymous – is paramount, because while law or self-regulation is lagging behind the speed of technology innovation, brands face an imperative to establish the correct processes and policies, which are critical to protect against data breaches or lawsuits that could critically damage a brand.

Today, many brands are laser focused on Millennials and the lifetime value they may bring. This generation grew up in the age of digital, where exploring, connecting and sharing across social media has not been a new, evolving experience; it is their norm. There is a misperception that because this generation grew up in the digital age, privacy, or lack thereof, is taken for granted – a risky and erroneous assumption. Remember, it's Millennials who created Snapchat to ensure their communications have a short shelf life, and this same generation is the savviest in controlling their privacy setting on sites like Facebook.

Consumer concerns about mobile are changing quickly with the advent of unique identifiers that raise red flags on collecting data on mobile, arguably the most personal, contextual and sensitive in nature. This should be a call to action for marketers – if you want to capitalize on the explosion of channels, devices and technologies that offer unprecedented opportunities to know your customers and delight them, you must be vigilant in your efforts to show consumers clear value, gaining and retaining the trust essential for your brand to grow and thrive.

Eleven
Understanding Risk

Consumer voice: uncoordinated and ubiquitous marketing can drive some consumers to resort to some or all of the following options to voice their concerns.

Ad Blockers

According to eMarketer more than 25 percent of U.S. internet users, 69.9 million people, will block ads in 2016. This is expected to increase in 2017.

The adoption of ad-blockers is driven more by the desire to speed up page loads to improve the digital experience, which is becoming increasingly disruptive with pop-up ads and clutter. While the impetus for adoption is not the protection of personal data from collection or use, the effects of ad-blocking significantly handicap advertisers and publishers with a shrinking audience and the inability to reach their audience and harness insights from audience engagements that enable brands and publishers to drive more relevant offers and services. In the next section we will outline how a better experience with a brand is created by delivering highly relevant, better targeted – but fewer – offers. That approach will lessen the adoption of ad-blockers; consumers simply want a better experience and a value exchange.

Ad Choices Opt-out

This option, introduced by the Digital Advertising Association (DAA) in 2011, disables internet-based advertising HTTP cookies on browsers.

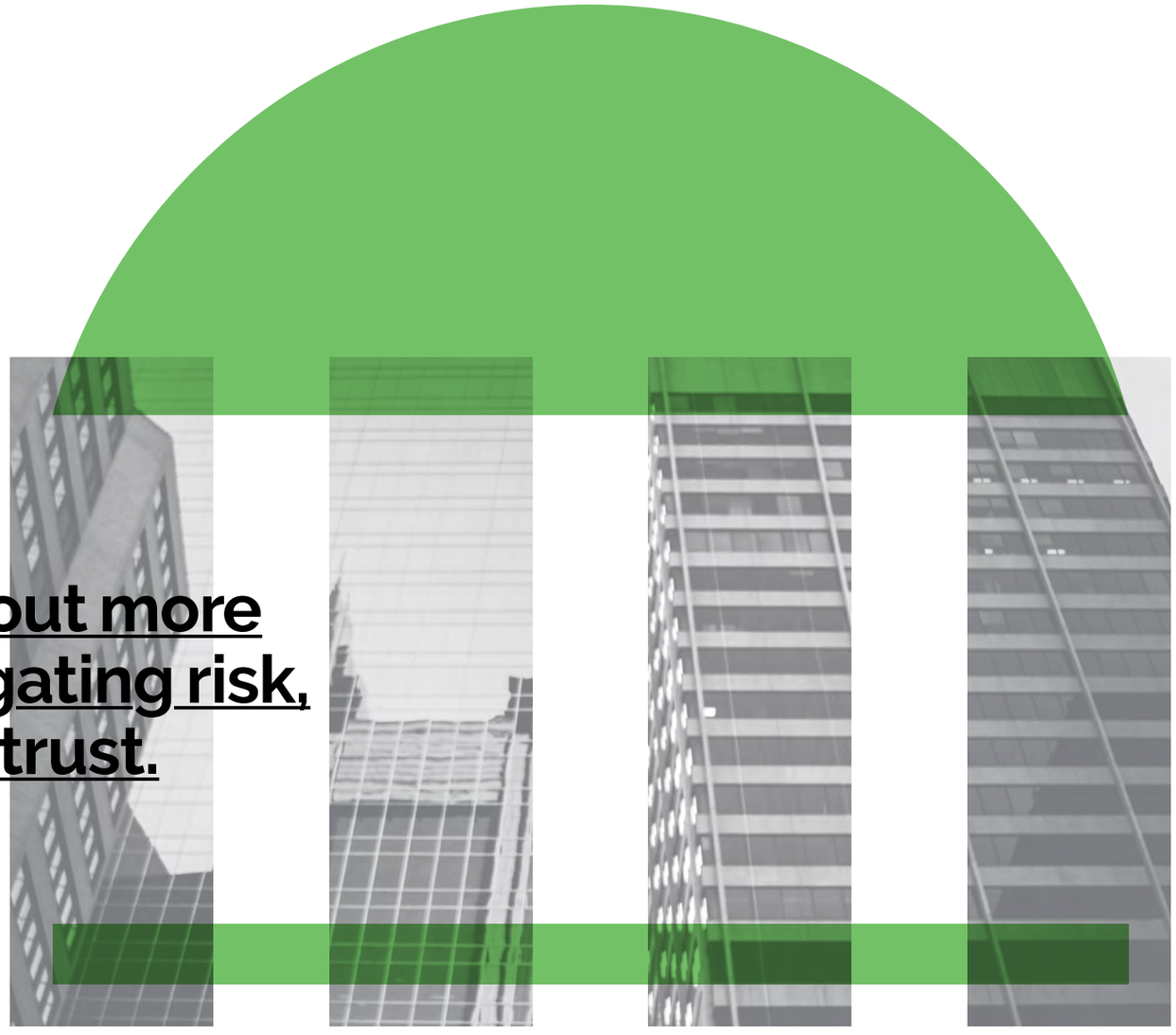
This will significantly decrease a brand's ability to identify and market to consumers based on data collected or inferred from their digital footprint.

Apps Choices Opt-out

This option is a mobile ad solution intended to complement Ad Choices, introduced by the DAA in February 2015. It provides consumers a downloadable app to opt out of advertising on mobile apps and in some cases to provide control for cross-device linking of data.

If the adoption of AppChoices accelerates it will further erode advertisers' ability to draw connections from the devices that are the most personal in nature and provide the most contextual data on a consumer's behavior and preferences.

Twelve
The Accountability Instinct



This is about more than mitigating risk, it's about trust.

Twelve
The Accountability Instinct

By the time this booklet is published, the discussion about the ethical use of data and the rules governing consumer privacy may have already evolved. Regulations may become tighter or looser, depending on the industry, geography or even specific corporate data governance policies. However, in these exciting and fast-moving times, some things remain constant – such as the tension between ideology and commercial interest, and that individuals are too often responsible for making a choice between potential risk and potential upside. Nor has it ever been (or ever will be) enough to focus on the law without thinking about what one should do.

The ethical consideration of data use may provide an interesting vantage point in driving a national conversation about corporate citizenry, humanism, perhaps even a renewed interest in those prescient Enlightenment theorists. But marketing leaders are business people, focused on business outcomes. So the focus should be on the ethical use of data as part of a business strategy that will lead to long-term success.

In exchange for their data, consumers expect marketers to use this newfound power responsibly and to always remember that as commercial users of data, we are tasked with creating real value for not only the enterprise, but also – and most importantly – for the consumer.

Marketers have never had a better opportunity to drive consumer engagement. They now have access to ever-increasing sources of data from every channel and device a consumer uses. Better still, the technology exists to connect and tie the signals consumers provide as they traverse the offline and online worlds back to known individuals. If brands can use this to build trust with the consumer through contextual, relevant and welcomed use of their data, responsible and robust data governance becomes a strategy where all parties benefit.

To square this circle, marketers need to develop the proper data use policies and processes. And then stick to them. Get this wrong and you run the risk of lost sales and, much worse, erosion of brand trust that will lose you customers for good. Get this right – consistently until such accountability almost becomes second nature – and you build brand trust and affinity that will earn you ironclad and sustained loyalty, historically the domain of the handful of marquee brands that have always put the customer at the center of everything they do.

This approach has the power to actually go beyond trust, affinity and loyalty creating brand evangelism moving beyond simple transactional engagement to truly engaged relationships.

The future of consumer engagement is fragile. Marketers must treat consumers' data as the most vital asset they own. If they can do that, relationships with consumers become a true value exchange, a promise we can all embrace.

Bios
Authors

Jennifer Barrett Glasgow, CIPP
Chief Privacy Officer Emeritus
Acxiom

Jennifer Barrett Glasgow was appointed Chief Privacy Officer in 1991, and over the course of her 25-year tenure, she developed Acxiom's global approach to information governance, compliance, consumer affairs, government affairs and related public relations. She also participated in numerous domestic and international efforts to develop information policy and industry codes of conduct.

In January 2016, she moved to Emeritus status where she now advises Acxiom on various strategic initiatives. She continues to be extremely active consulting with clients and advising policy makers about the ethical use of information and is a regular speaker at both public and private sector events, Jennifer serves on the U.S. Direct Marketing Association Board of Directors and its Privacy Shield Arbitration Committee.

In 2011, the International Association of Privacy Professionals (IAPP), an association of more than 25,000 members worldwide, recognized Jennifer as its Vanguard winner, the highest recognition given for leadership, knowledge and involvement in the profession.

Sheila Colclasure
Chief Global Privacy and Public Policy Officer
Acxiom and LiveRamp

Since 1998, Sheila has worked to develop and implement policy and practice for Acxiom's Privacy and Public Policy Program. In January 2016, Sheila was appointed Chief Global Privacy and Public Policy Officer for Acxiom and LiveRamp and directs all information use policies, compliance, consumer affairs, government affairs and related public relations for Acxiom's and LiveRamp's operations globally.

Prior to joining Acxiom, Sheila worked for the U.S. Senate and then managed congressional and political affairs for the American Institute of Certified Public Accountants in its Washington, D.C. office, focusing on legislative and regulatory initiatives as well as directing its political action committee. Sheila has a master's degree in communications, specializing in business and political communication.

Today Sheila functions as corporate liaison to several industry standards-setting groups and research and policy development groups. She participates in numerous domestic and international efforts to help develop effective public policy, establish industry best practices and achieve maximum harmonization of information policy across the world. With extensive knowledge of laws governing the collection and use of information worldwide, she is sought out by policy makers, regulators and government agencies for her views on the ethical use of data.

Acxiom is a global leader in data governance, Ethical Data Use by Design implementation, and data privacy best practices. We help enterprises achieve demonstrable compliance with all industry and government regulations through assessments, education and strategic consulting that enable marketing leaders to safely activate their data and strengthen connections between people, businesses and their partners.

acxiom™

Acxiom provides the data foundation for the world's best marketers. We enable people-based marketing everywhere through a simple, open approach to connecting systems and data that drives seamless customer experiences and higher ROI. A leader in the ethical use of data for more than 45 years, Acxiom helps thousands of clients and partners around the globe work together to create a world where all marketing is relevant.

www.acxiom.com

acxiom™