POSSIBLENOW™

Consent, Preferences, Insights, Compliance

TRUST
Be Human

MAKING THE CASE FOR CONSENT AND PREFERENCE MANAGEMENT

By Danny Hitt, Vice President of Sales

We empower the individual's voice, so trust is built, and relationships are enriched.

WHAT'S INSIDE

Establishing the Need for Consent and Preference Management

According to a recent Accenture survey, more than 70 percent of consumers prefer to do business with brands that use personal information to make their shopping experiences more relevant. This should come as no surprise to anyone leading an enterprise-level company in the modern age. In survey after survey, study after study, consumers around the globe are demanding personalization, privacy, and the power to control the conversation with the brands that serve them.

For many CMOs and CTOs, the challenge is not in proving or establishing the need to address privacy, personalization, and increasing demands for interaction. Rather, the challenge lies in establishing the best method for achieving success.

The dilemma is further complicated by language used to define the relationship between consumer and company in the digital age. The line between customer engagement and customer experience is blurry at best, and neither priority holds a clear mandate over traditional corporate structure. Is the marketing department in charge of engagement? Is customer service in charge of experience? Is IT shared by both groups or managed according to an entirely separate structure and vision?

A North Highland survey of 700 senior business leaders found 87 percent agree that "customer experience" is the top strategic priority for driving growth. However, only one-in-three said they felt prepared to take on a customer experience initiative.

Why? The goal is too large, too vague, and involves too many moving parts. The senior executives surveyed by North Highland know they need to listen to customers and engage them in meaningful, profitable relationships. But they haven't figured out how to break customer experience or engagement down into actionable pieces. Without a concrete plan, it becomes almost impossible to earn approval from IT, legal, investor relations, or other stakeholders for many worthwhile initiatives.

The best starting point for an enterprise is the management of zero-party data: customer consents, insights, and preferences (the active collection, maintenance and distribution of unique consumer characteristics, such as product interest, channel preference and frequency of communication). Executed correctly, a robust zero-party data management program can power the personalization, privacy, and interactivity modern consumers demand. A zero-party data management initiative for customer consents and preferences is a tangible project with a specific action plan and set of goals to improve both experience and engagement.

The following pages will demonstrate how consent and preference management can be defined to internal decision-makers, framed for budgeting, communicated to collaborating stakeholders and ultimately approved for action.

Defining the Benefits of Consent and Preference Management

The case for consent and preference management is typically organized into two clear categories:

A) strengthening compliance with privacy regulations and

B) improving customer relationships, increasing customer lifetime ROI.

Each would present a compelling case on its own. But considered together, addressing both with one solution offers a strong, evidence and return on investment-based position from which to move an organization towards the active collection, maintenance, and distribution of zero-party data - namely, customer consents, preferences, and insights.

> "Businesses crave insight into the context in which consumers are using their products - and consumers want businesses to deliver contextually relevant services." - Fatemah Khatibloo, Forrester Research

Stronger compliance and privacy protection

Recent research has shown that 77 percent of US adults agree that it has become more difficult to trust what companies say and do, 54 percent of consumers believe that companies do not operate with their best interests in mind, and 57 percent of customers will stop doing business with a company entirely because they've lost trust in the company.

In response, regulators and legislators around the globe began working quickly to introduce legislation such as the EU's General Data Protection Regulation (GDPR), the United States' Telephone Consumer Protection Act (TCPA), Canada's Anti-Spam Law (CASL), and others, to enhance privacy protections and address widespread consumer concerns about data and identity theft, unwanted communications, and behavior tracking.

For example, regulations such as the GDPR requires marketers to give strong consideration to obtaining and maintaining strict permissions in order to communicate with any citizen of the EU. Central to the regulation is a high standard for consent and fines as great as 20 million euros or four percent of total worldwide annual revenue, whichever is larger.

The TCPA requires companies to collect consent prior to calling or sending text messages to mobile devices. Fines for sending text messages without first obtaining express written consent range from $500-$1500 per text message sent. With a recent rise in class action lawsuits, these fines can add up quickly, with companies like Jiffy Lube being fined $47 million for their TCPA violations.

CASL requires consent prior to sending commercial electronic messages such as emails and text messages and carries penalties of up to $1 million for individuals and $10 million for corporations per violation. If a company hasn't earned consent and has no means by which to gain consent, it faces the daunting decision of either losing a contact due to privacy concerns or facing significant liability.

Zero-party data collection represents a critical opportunity to earn consent and protect the right to interact with a consumer. Moreover, appropriate storage and maintenance of such data through an active consent and preferences management program protects its legal authority when challenged.

Improved marketing ROI

By reducing opt-outs and increasing opt-ins, the overall size of the marketable audience grows. With the implementation of a simple opt-down system — a component of a preference management solution accessed through an email unsubscribe link — PossibleNOW customers see an average of 60 and 90 percent fewer opt-outs.

In addition to preserving the pool of prospects, the ongoing collection of consent and preference data reveals new opportunities will emerge that marketers can proactively leverage to their advantage. For a clothing retailer, understanding customer insights along with product interest and channel of choice could result in a seasonal swimwear promotion via email instead of an expensive and marginally effective one-size-fits-all brochure or catalog.

Finally, the collection and management of consent and preferences for zero-party data allows CMOs to shift staff time and budget dollars from guesswork to fact-based decision-making. A marketing team that only has access to purchase history and customer shipping addresses trend towards broad, one-size-fits-all campaigns, often with discouraging results. Customer insights data gives the customer a voice in the type of communications they want to receive and empowering niche campaigns that address stated needs at timely intervals.

Presented together, the broad compliance and marketing benefits of consent and preference management offer a compelling case for consideration. Risk mitigation has become an important part of the CMO job description and the management of zero-party data like customer consent and preferences addresses a number of its critical challenges. It's also the key to building customer trust, facilitating lasting customer engagement and real-time responsiveness with rich, marketable data that powers campaigns and delivers bottom-line results.

> "The typical terms of agreement that we check when we want to use the services of an Internet company invariably give the company the right to redeploy our information for their own benefit. Some companies also give consumers the right to opt-out of that information-gathering, but it is usually a process that requires some effort. A far better approach would be customers opting in instead of opting out."
>
> - **Joe Nocera, The New York Times**

Framing the Decision: Build vs Buy

With the need for zero-party data management established and its benefits defined, many organizations face a growing dilemma of awareness – is it something we must engage a third party to implement or can we build it internally? It's a complicated but necessary question that should include each of the considerations listed here:

Consideration	In-house	Outsourced
Subject matter expertise	What resources do you have in-house?	Expert providers think about customer data collection and management every day from all perspectives; customer engagement, privacy, technology, etc
Are resources available? Is there a risk that they will be pulled off the project?	If you have in-house resources, are you willing and able to commit them to this project on an ongoing basis to implement and maintain the system?	Resources are available & have experience implementing and maintaining solutions with both feature updates & compliance requirements.
When do you need it deployed?	Design, development, and deployment can take 2 to 3 years. Have you created a timeline for this project?	Typical deployments take 3 to 6 months
Can you absorb the expense?	Large up front capital expense of $5 to $20 million is common. Have you estimated the cost of your project?	Typical implementation fees are relatively small since the solution is built out.
Are your systems designed to house and archive customer zero-party data?	CRMs, Marketing Automation, Marketing Databases – No	Yes
Can you centralize your zero-party data, including customer consents and preferences?	?	Yes
Can it be designed to easily set up new programs?	?	Yes
Can you develop an API toolset to share data across the organization?	?	Yes
Can you develop configurable reports?	?	Yes
Can you develop a validation and alert process?	?	Yes
Can you develop comprehensive data collection and delivery?	?	Yes

Fostering Internal Consensus

Implementation of zero-party data management in an enterprise environment requires a rigorous, multi-party justification process. In this respect, it mirrors a familiar pattern whereby an enterprise considers a new technology that holds the potential to impact or even transform many of its legacy processes and systems.

In the case of zero-party data management, the dynamic is influenced by previous efforts or research into the question. Almost without exception, enterprise organizations already have certain customer data management tools in place and have studied or considered its broader implications. In any case, the challenge of fostering internal consensus begins with solving certain foundational questions:

What is the enterprise doing to collect, maintain, and distribute customer zero-party data, such as customer consents and preferences?

The answer may lie in sales, support, marketing, IT or all of the above. In many cases, siloed departments hold their own data interaction models or rely on limited zero-party data management tools via an Email Service Provider (ESP), a marketing agency, or other third party. Uncover all of the different systems and processes that should be considered as part of a consent and preference management solution by understanding what communications are being sent to what customers and why.

What does the enterprise's leadership think it is doing to collect, maintain, and distribute customer zero-party data, such as customer consents and preferences?

The distance between perception and reality is critical in framing the larger implementation question. Confusion over terminology, departmental authority, what is included as part of zero-party data, how data collection is deployed, or exposure to risk, if unforeseen by those recommending a zero-party data management initiative, can lead to costly and unnecessary delays.

Who are the necessary partners for implementation of zero-party data management, even on a limited scale?

With reliable information in hand on the perception and reality of existing efforts, a useful effort can be made to identify key partnerships that the management of customer consents and preferences (and all customer zero-party data) will require in order to move forward.

Through an exploration of these foundational questions, the consent and preference management "champion" within the organization should be prepared to introduce the topic from an actionable position.

Key steps for implementing a zero-party data management platform:

- Identify a problem that needs to be solved or opportunity with upside potential
- Establish a project team
- Determine present state and outcome goals
- Prepare rollout plan
- Measure results
- Conduct post mortem and identify areas for improvement
- Report results to management team
- Begin phase II

Conclusion: Moving from Discussion to Action

Here's an all-too familiar scenario: senior leadership recognizes the need for better, more efficient customer engagement and understands that a sophisticated solution for managing zero-party data is a necessary prerequisite to achieving that goal. Consent and preference management is listed as a specific priority and handed to IT for a feasibility and cost study. The study reveals significant challenges and results in a gloomy report that it is prohibitively expensive, requires an unreasonable timetable, or is deemed impossible given the enterprise's current infrastructure. Discouraged by the result, senior leadership shelves the initiative, only to return to it during the next budget/planning cycle.

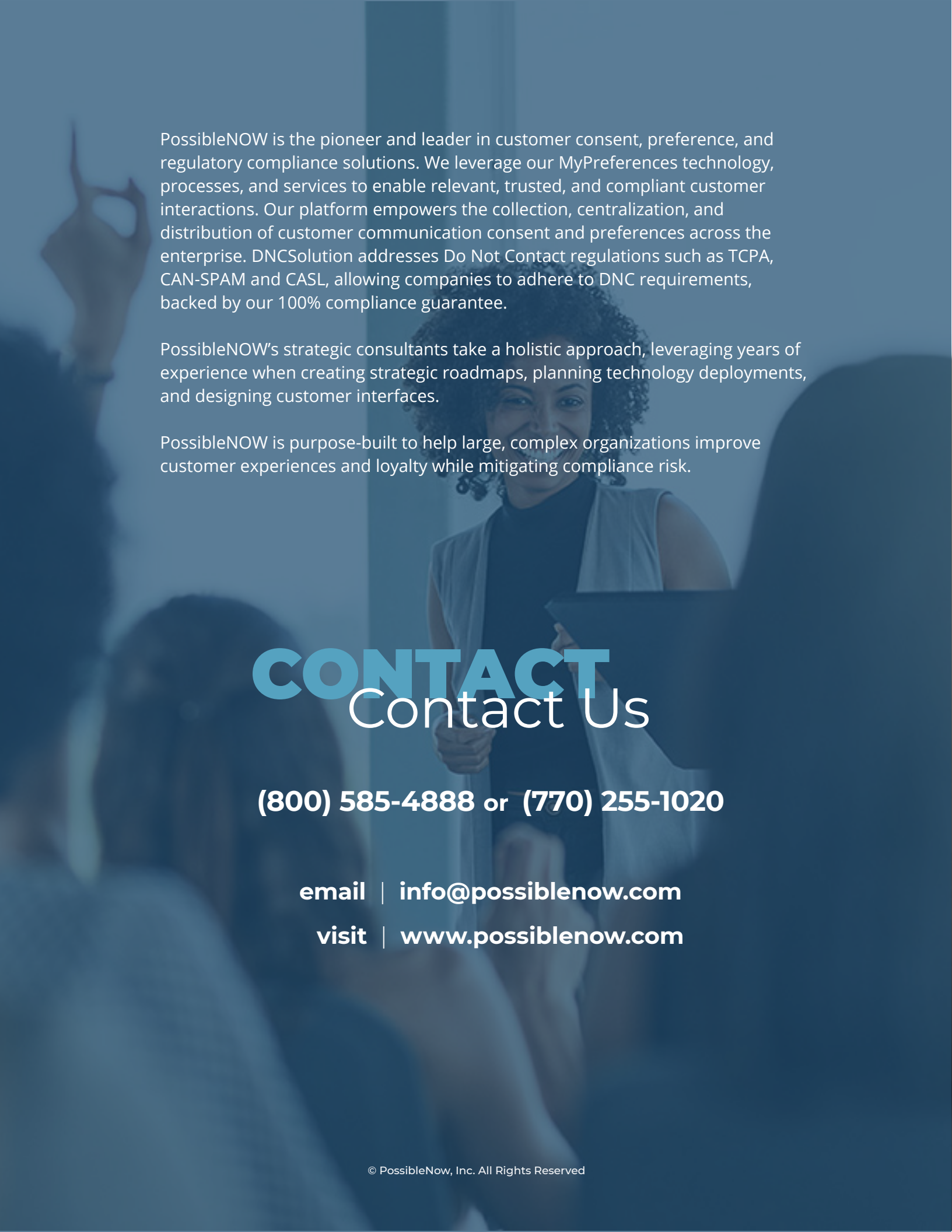
It's an unfortunate pattern but one that can be broken. The key, in many cases, is creating a smaller goal and letting the consent and preference management initiative prove itself prior to larger investment or broader expansion. Here are three simple actions (offered in order of complexity) that can actually be proposed, piloted, budgeted, and achieved quickly:

1. Offer opt-down functionality in your email marketing:
   Instead of presenting customers with an all-or-nothing engagement, give them the power to tailor communications to suit their interests. Offering an opt-down option drastically reduces opt-outs and helps marketers focus messaging on topics of interest.

2. Install a website trust and preference center:
   Create an easy-to-use portal where prospects and customers can create individual profiles, give or revoke their consent to be contact, select topics of interest, preferred delivery channels, and pace of communications. Centers of this kind provide the ability for customers to provide their insights and maintain their preferences as their interests change over time.

3. Expand your zero-party data collection with a limited starter program:
   Zero-party data management should be present at every interaction point between brand and customer, such as mobile, social media, in-store, contact center and more. However, these initiatives require approval from many stakeholders and can quickly become bogged down or even abandoned. Identify a specific brand or line of business to use as a starter program to prove zero-party data management ROI and gain momentum before seeking company-wide application.

Approaching zero-party data management as a series of actionable steps makes it easier to plan and earn organizational buy-in, beginning with consent and preference management. The challenge of making the case for zero-party data management in an enterprise environment can be complex and multi-faceted. In many ways, it quickly becomes a process of simplification — clear delineation of what it is, why it is important, and how to begin.



PossibleNOW is the pioneer and leader in customer consent, preference, and regulatory compliance solutions. We leverage our MyPreferences technology, processes, and services to enable relevant, trusted, and compliant customer interactions. Our platform empowers the collection, centralization, and distribution of customer communication consent and preferences across the enterprise. DNCSolution addresses Do Not Contact regulations such as TCPA, CAN-SPAM and CASL, allowing companies to adhere to DNC requirements, backed by our 100% compliance guarantee.

PossibleNOW's strategic consultants take a holistic approach, leveraging years of experience when creating strategic roadmaps, planning technology deployments, and designing customer interfaces.

PossibleNOW is purpose-built to help large, complex organizations improve customer experiences and loyalty while mitigating compliance risk.

CONTACT

Contact Us

(800) 585-4888 or (770) 255-1020

email | info@possiblenow.com

visit | www.possiblenow.com