

Surviving and Thriving in the Opt-Out World

Challenges and Opportunities for Marketers

The Opt-Out World:
76% of adult
Americans say they
have added their
numbers to the
National Do Not Call
Registry.

Today more than ever, consumers and businesses understand their rights to privacy and to refuse the presentation of marketing messages. Case in point: over 150 million phone numbers have been added to the National Do Not Call Registry since it was established in 2003. Consumers and businesses also know they can opt-out of email campaigns and refuse permission for companies to share their information.

As a result, the pool of prospects that marketers can freely contact has shrunk dramatically. This restricted environment has aptly been called the "opt-out world."

The Scope of the Problem

The requirement to track privacy preferences is not new. For over a decade, various state and federal regulations have mandated that companies maintain do-not-contact lists. Further complicating the picture, the regulations allow various exemptions to opt-outs, notably in the case of established business relationships (EBRs).

To meet legal requirements, marketers have built procedures to collect and store privacy preference data, and to prevent unauthorized contacts to customers and prospects. Savvy marketers have also taken a proactive approach, using opt-in campaigns and other permission marketing techniques.

But these initiatives are often hampered by the volume and complexity of the data. To create compliant campaigns, marketers must not only maintain call, fax, mail, email, and share preferences for all of their contacts, but must correctly evaluate multiple possible opt-outs, opt-ins, and exemptions for each contact record.

For large organizations, properly managing privacy preferences is an even more formidable challenge. An enterprise has many moving parts to its data sources and marketing channels. Privacy preferences must be collected and accessed by corporate operations, branch offices, field agents, and vendors. Privacy designations may reside in the enterprise data warehouse, CRM system, marketing databases and other repositories.

Large companies typically manage multiple brands and business units with separate marketing departments. Many companies have grown by acquisition and end up holding disparate collections of privacy data. Information often exists in silos, inaccessible to many of the people throughout the enterprise who need it.

As a result, marketers often fail to leverage opt-ins and exemptions they could legitimately use if the data were shared. Worse, they may claim exemptions they are unable to substantiate, or execute marketing campaigns that are not fully compliant. Companies found in violation of privacy and do not contact laws face stiff fines and damaging exposure in the media. In 2007 for example, a major home security company was

The Risks of Non-Compliance:

In 2007, a major home security company was fined \$2 million by the FTC for violation of Do Not Call laws.

fined two million dollars by the Federal Trade Commission for calling phone numbers on the National Do Not Call Registry.

Some Partial Solutions

The technology and marketing services industries have made various attempts to address the challenges of the opt-out world. These partial solutions fall into several categories.

Regulatory Guides - Several publishers compile do not contact databases from state, federal and third-party sources. These guides are typically available by subscription over the Web. They require marketers to look up contact records and compile their own lists.

List Scrubbing Tools - With these solutions, marketers submit files of contact records, which are then compared to national and state do not contact lists. Records found to be on the lists are removed or "scrubbed" from the marketer's file. While helpful in maintaining compliance with government and third-party opt-out lists, these tools require the marketers to maintain their own files. They also do not manage opt-out requests made directly to a company; nor do they handle opt-ins or exemptions.

Call-Blocking Systems - This class of solution interfaces to a call-center's telephone network. It automatically blocks outgoing calls to numbers that are on Do Not Call lists. While useful for call centers, these systems require a company to maintain its own lists of contactable numbers. They do not address email, mail or the sharing of information.

CRM Systems - Some organizations attempt to manage privacy preferences using their Customer Relationship Management system. As these systems are not designed for privacy data, this approach requires custom programming and re-architecting of databases. The problem of collecting "siloed" data from disparate sources remains, as does the challenge of integrating third-party opt-out lists and of properly evaluating opt-ins and exemptions.

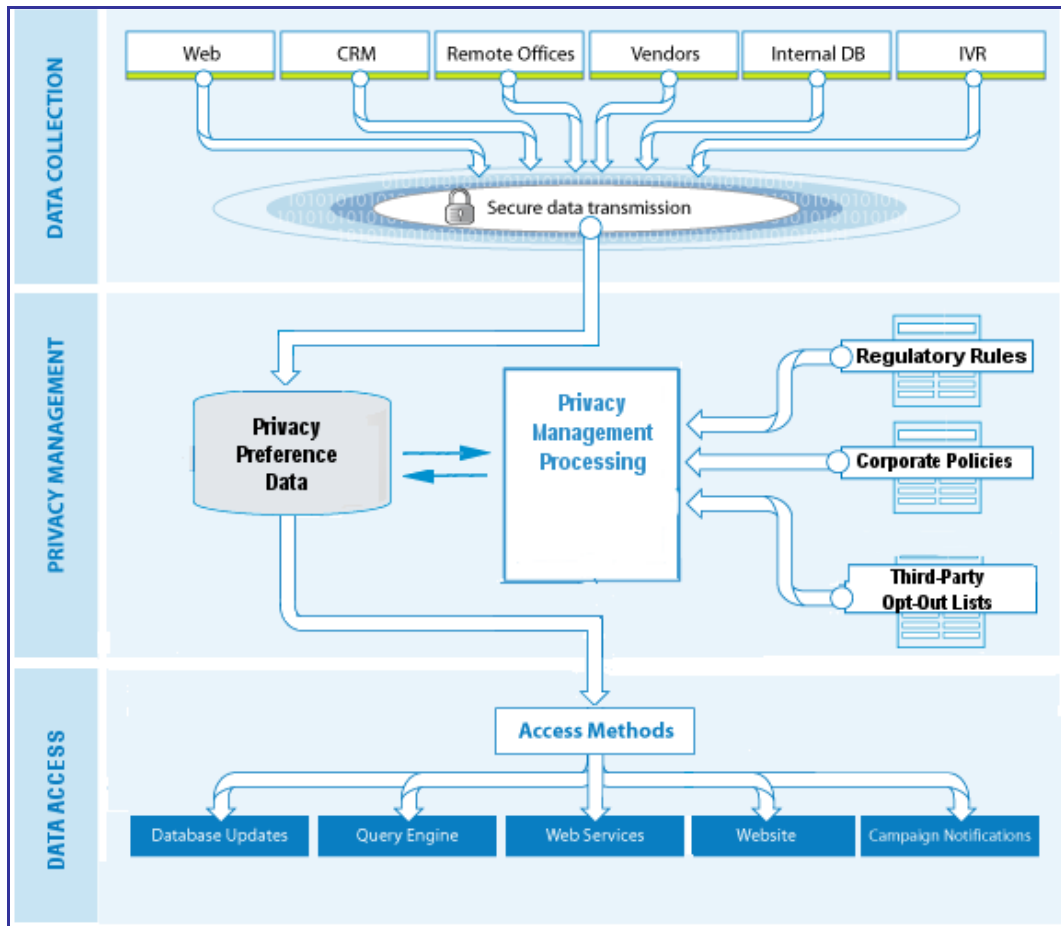
Centralized Privacy Data Management

Given the complexity of the challenges and the incomplete solutions developed so far, many marketers have come to favor a comprehensive, unified approach. They envision a next-generation solution in the form of a **centralized repository of privacy preference data**.

As illustrated in the Figure, the centralized system manages privacy designations for every customer and prospect known to the enterprise. It is flexible enough to collect opt-ins and opt-outs from all available sources, both within the company and from third-party list aggregators. It processes contact records—balancing opt-ins, opt-outs and exemptions—to define the "contactable status" of each record. It then feeds this status information to all of the enterprise channels that need it.

Next Generation

Solution: *The centralized system manages privacy designations for every customer and prospect known to the enterprise.*



A Centralized Solution for Privacy Data Management

Data Collection

The repository collects privacy preference data from sources across the enterprise. These include existing databases as well as real-time channels, such as web pages or IVR systems where consumers or third-party vendors might enter privacy preferences. Updates occur both in real-time and via batch processing. The data is securely transmitted into the system.

Privacy Management

Contact records are stored in a central database. They are continuously evaluated in terms of regulatory requirements, corporate policies and the latest versions of third-party opt-out lists (state, federal and others, such as those published by the Direct Marketing Association). This processing maintains the correct **contactable and shareable status** of each contact record.

The privacy status information tracked by the system can be as simple as "opted in" or "opted out." Or, it can be very detailed, listing a person's preferences as to methods of contact, days and times, frequencies, or permissions to be contacted about particular products or services only.

Data Access

The system dispenses the validated, up-to-date privacy status information to everyone who needs it throughout the enterprise. Web pages can be used to check on the current status of any record. Marketers can query their own databases or the central repository to compile lists of valid contacts for their campaigns.

Key Benefits

Through the centralized approach to privacy data management, marketers and their companies stand to realize important benefits:

- **Up-to-date information** - Privacy designations within the enterprise can be updated daily. Third-party opt-out lists and state and federal regulatory requirements can be reliably updated whenever changes are published.
- **Maximum number of fully-compliant contacts** - The system accurately analyzes conditional opt-ins and exemptions to maximize the number of customers and prospects who can safely be contacted for any marketing initiative. Standardized contactable guidelines are enforced across the enterprise.
- **Automated campaign creation and notifications** - Queries can be used to specify the requirements for a marketing campaign and automatically generate lists of valid contacts. Because the data is stored in one place and frequently updated, the system can update campaign lists and send out notifications when someone's privacy status changes.
- **Dependable archiving and reporting** - Marketers can display the contactable status of any consumer record at any point in time. The system thus supports past marketing decisions and proves compliance to regulators if the need arises.

Fully Compliant Contacts:

The system analyzes conditional opt-ins and exemptions to maximize the number of customers and prospect who can safely be contacted.

Centralized Privacy Data Management is an emerging solution that promises significant advantages. Backed by efficient software and sound policy decisions, the centralized privacy repository equips marketers to survive and thrive in the opt-out world.

About <Company>

Client company description and contact information, removed from this portfolio sample.