

Overcome Email Marketing Privacy Challenges:

DELIGHT CUSTOMERS. PROTECT YOUR ORGANIZATION.

Marketo®

The Changing Face of Digital Privacy

The past few years have seen unprecedented changes in consumer buying habits. Consumers demand instant gratification and many are willing to share some personal information in exchange. But at the same time, buyers are getting smarter about what they are willing to share.

Typically, consumers are wary of sharing their email addresses and other personal details if they:

- Don't know how their information will be used
- Aren't sure how many messages they'll receive
- Would rather research products themselves, rather than interact with a salesperson

Consumers don't want to get spammed, and they're very concerned about identity theft. Recent disclosures of governmental privacy oversteps around the globe have made personal data seem more vulnerable than ever before. These conditions are making the email marketer's job harder every day, but the good news is that proactive, progressive email marketers can use the current digital privacy climate to their advantage.

In this ebook, we'll explain how marketers can navigate the cultural backlash against information sharing, and fully understand upcoming changes to laws governing email and cookie collection.



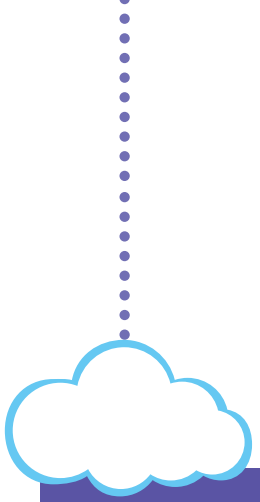
What's the Big Deal About Privacy?

Today, we live in a world where people share the most intimate moments of their lives with hundreds or even thousands of people through social media. It sometimes seems like nothing is private – we'll advertise our moods, our relationship status, and our job woes to anyone who will listen on Facebook, Twitter, Instagram, and beyond.

We're also vastly more willing to input our credit card information online than we were a decade ago. Where we once thought it a novelty to have a book drop-shipped to us from another state, we're now comfortable buying our toothpaste on our laptop. We habitually give ecommerce sites permission to store our credit card numbers and other sensitive information in their secure databases. We're even transmitting our tax information over the internet. The barriers to uploading our sensitive personal info have been virtually dissolved.

So why worry about privacy?

Email privacy is about permission. Consumers want full control of which information they give us and how we use it. Granting us access to their credit card numbers so they can easily make purchases is one thing; when we use their email addresses to send them information without their consent, that's another.



Marketers need to comply with two sets of expectations:

1. What consumers are aware of and want
2. What the law requires us to do

As marketers, we own the growth agenda.

Shifts in buyer habits have already significantly restructured today's organization: marketing is now more responsible for revenue than ever before. In large part, this is because consumers have gotten savvy about educating themselves before they ever approach us to buy. Our marketing messages serve as research for consumers, who (thanks to the internet) have a library of information available at their fingertips. As a crucial source of product information and a first-touch point, marketing can make or break a consumer's relationship with a brand.

"With great power comes great responsibility."

As Spider-Man taught us, if we are to succeed in our (marketing) mission, we must be prepared to meet the responsibilities of our powerful new role. And that means considering the legal implications of our tactics as well as their marketing impact. With this in mind, how can we:

- **Responsibly use our tools and technologies to build trust with customers**
- **Comply with privacy legislation to protect our companies in all relevant global markets**

It's a balancing act, and marketers have to be knowledgeable and nimble.

According to Forrester Research, consumers complete about

70%

of their buying cycle before conversing with salespeople.



The New Rules of Email Marketing Engagement

Betraying a consumer's trust is the kiss of death for marketers. This is a lesson we've learned the hard way as we've been given more and more access to consumers' private information. You can send a thousand welcome email messages to a consumer, but if he perceives just one to be spam, he'll remove himself from your list very quickly. Consumers are sensitive, and privacy is their paramount concern.

Luckily, new developments and technological improvements have helped email marketers develop more relevant, personalized ways to communicate with their audiences than ever before. But these new capabilities should be exercised cautiously — if they aren't, you risk invading the privacy of your audience.

No one wants to get "red flagged," but simply laying off on email doesn't serve you as a marketer. The key to keeping your customers and prospects engaged and on your side? Use your email marketing to build relationships over time, always staying keenly attuned to where each customer is in his particular buying cycle.

Building relationships over time looks something like this:

1. **From Finding Customers to Being Found**
   Use content marketing and inbound marketing to build trust and keep your audience from feeling overwhelmed.

2. **From Point-in-Time Blasts to 1:1 Durable Relationships**
   Create lasting relationships by engaging customers and listening to their needs. Use demographic and behavioral segmentation to build solid relationships, which will make people more comfortable sharing information.

3. **From a Few Isolated Channels to an Integrated Explosion**
   Today's consumer constantly shifts contexts, from email to social channels to in-person events. Your marketing strategy must meet your audiences where they are, in a consistent way. Consistency builds trust.

4. **From Intuitive Decision-Making to Owned, Big-Time Series Data**
   Use the data you collect to make intelligent and informed marketing decisions.

Everyone Can Market Like Amazon.com

The key to relationship marketing today is to use consumers' private information respectfully. Using data in a way that benefits both the consumer and the marketer is nothing new.

Amazon.com has successfully done this for years, leveraging data to provide personalized recommendations when customers visit their site. By tracking visitor search and buying habits, Amazon.com – and so many other retailers – use big data to create a unique and intimate experience for each and every customer.

If you want your audience to willingly relinquish their information, you should use that information to understand how customers are engaging with your brand or products, and then to make suggestions and recommendations.

This now ubiquitous marketing tactic might seem counterintuitive when we're talking about privacy laws. But experience and metrics show us that consumers actually like being marketed to on a personal level. They find Amazon.com-like recommendation engines to be convenient mind-readers that make their buying lives easier. The key to the success of recommendation engines is that they push products and offers to consumers at ***an appropriate time and place.***

The ability to wield big data well is not just the domain of behemoths like Amazon.com. Today, every marketer of every company of every size has the ability to market this way. In fact, customers expect it.

Don't Overstep Your Bounds

Just because we can gather data about consumers doesn't mean it's always wise to use it. To overstep your bounds as a marketer is to risk the "creep" factor — and more and more, to incur legal penalties that put your organization's reputation and profit margins at risk.

As we look to the future, we see a perfect storm of privacy challenges brewing: more regulation, stricter enforcement, and stronger consumer preferences to abide by. In this environment, privacy practices are the marketer's friend, providing a set of rules we can follow so we can successfully navigate these changes.

The Legal Side: What are the Regulations?

Ignorance of today's privacy laws puts you at greater risk than ever before. Enforcement is up, and new regulations raise the stakes for sending unsolicited email and tracking people online without their knowledge.

North American Privacy Law Changes

State by state, the US is cracking down on electronic privacy. Many states, like Nebraska and Pennsylvania, are carefully enforcing privacy policy verbiage, ensuring that such policies never contain "false and misleading statements." Connecticut, Delaware, Colorado, and Tennessee have established strict rules around how employers can monitor employee email communications and internet activity. The most stringent laws — and the ones that most pertain to marketers — currently come from Canada and California:

Canada's CASL Email Law

Effective July 1, 2014, this law requires specific opt-in methods for sending emails, and prohibits the types of pre-checked opt-in boxes that formerly accompanied purchase decisions. Under this new law, violators can be sued by individual email recipients. Telephone and in-person opt-in methods require you to record the relevant in-person or phone conversation. For electronic opt-in policies, you must record:

- **The URL where the person filled out the opt-in form**
- **A time stamp**
- **Their login IP address**



In addition, you will only be able to email consumers for six months after they inquire about your services, or for two years if they are a former customer.

California's Privacy Law AB370

In 2013, Californians began requiring global organizations to review how they track online visitors to their websites. The amendment to the California Online Privacy Protection Act of 2003 requires website owners to:

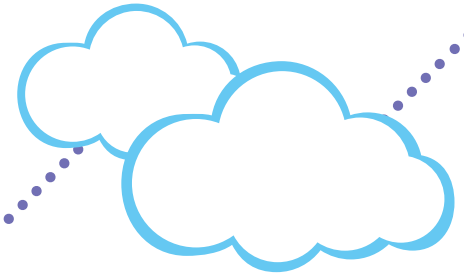
- Disclose whether or not they respect "Do Not Track" browser settings
- Disclose whether or not third parties collect personally identifiable information about visitors for them
- Have a comprehensive privacy policy

The EU's General Data Protection Regulation (GDPR)

The European Union is currently revamping its already restrictive privacy laws. The General Data Protection Regulation (GDPR) may go into effect by 2016, requiring companies to think carefully about how they acquire people's consent to receive communication.

Here are some notable highlights of the GDPR, which also appear in other emerging laws:

- **Breach notification:** Requires that you disclose any data loss incidents, with fines of up to €1 million, or 2% of the global annual turnover, imposed by the Data Protection Authority (DPA).
- **Privacy processes:** Privacy impact assessment and policy requirements
- **A rise in the age of consent:** From 13 to 18 for consumers to give their consent to opt in.
- **Right to be forgotten:** Consumers can request that you permanently delete their information, including data, photos, and links.
- **Processor controller obligations:** Demands stronger organizational responsibility for data security. The DPA will now be considered the "lead authority" when it comes to monitoring data processed by businesses.
- **Hardened consent rules:** Permission requirements for using personal data have also tightened. Assuming consent from a "data subject's" silence will no longer be permissible; instead, consent must be given in a statement or by an affirmative action such as checking a consent box.



APAC Privacy Legislation

Since 2012, privacy laws in the Asia Pacific (APAC) Region have grown significantly stronger. Australia, Hong Kong, and Singapore have all notably introduced new legislation which seeks to:

1. **Protect individuals from illegal transfers of data**

2. **Create much higher fines for breaches of direct marketing rules and unauthorized disclosure of data**

2014 has seen the enactment of many new provisions, including Singapore's Do Not Call registry and Australia's complete revision of their Privacy Act 1988. Violations of Hong Kong's data privacy laws can earn offenders fines of up to HK $1 million (or US $129,000), and Japan is predicted to make major changes to its privacy laws in 2015.

The new Australian Privacy Principles (APPs) serve to highlight some common themes that all marketers should be aware of, even outside of APAC. Principle 7 requires marketers to ensure that in each direct marketing communication with the individual, the organization includes a prominent 'opt-out' statement that draws the individual's attention to their no-marketing rights.

This theme of greater transparency and increased prominence of information rights is very much mirrored in the new EU Privacy Regulation. These principles and regulations are not to be ignored!

The Consumer Side: How Your Audience Feels About Privacy

In the courtroom of public opinion, privacy can be a messy business. But email privacy isn't just about the law — it's also about how your audience perceives their own boundaries. Here's the breakdown of consumers' relationship to privacy:

Exhibit A: The Quantified Self

Today, people use technology to track everything from their sleep habits to how many steps they take a day. There's even a contact lens that alerts insulin users to rises in blood sugar levels. All the data these technologies generate can help companies communicate with customers — to send them content that makes them say, "Wow, that message is for me!"

Exhibit B: The Creep Factor

Remember the story of the father who demanded an apology from Target after they sent his teenage daughter coupons for baby gear… and then found out his little girl had some big news? What sometimes masquerades as relationship marketing can feel like stalking and manipulation, which backfires big time. Target would have been well-served to do a little bit of investigative work into certain sectors of their audience before enthusiastically emailing off sensitive marketing messages.

Exhibit C: Consumer Consciousness

If you've ever signed up for a store club card or registered with a website, you have to know that companies track your behaviors and put that data to use…right? Not necessarily. A recent study from the Direct Marketing Association in the U.K. found that only about 20% of respondents are fully aware of how companies track online behaviors and preferences. Around 80% are somewhat aware of those techniques, but that number rises with each revelation about a new privacy invasion, whether it comes from the government, a hacker, or a business.

Exhibit D: Stealth Wear for Your Phone

The bar of awareness is definitely rising. Designer Adam Harvey made national news in 2013 with his line of Stealth Wear, clothing designed to protect the wearer from detection and surveillance. His Off Pocket anti-tracking phone cover, a privacy case that can take your phone completely off the grid and render you virtually invisible, flies off the shelves.

The success of these types of products indicates that as people become more aware of the various ways they're being tracked, they also become more guarded. For brands to gain trust, we have to explain exactly what we plan to do with data. And we have to make sharing the consumer's choice.

So how do we make a winning case? By building trust with every email marketing move. Trust is critical to consumer-marketer relationships. According to Direct Marketing Association, 58% of consumers cite trust as the most important factor when deciding whether or not to share information.

While it's true that consumers will always ask what they'll get out of a marketing interaction, the answer only matters if the consumer trusts the marketer. The buyer won't be motivated by an incentive if his trust will be betrayed in the process. And consumers don't tend to give second chances.

How Organizations Can Protect Their Buyers and Themselves

Now that you're in the know, it's important that you're protecting both your buyer's privacy and your own legality. Here are some voluntary steps that will get you in line with upcoming privacy changes:

1. **"Trust Me" seals.**
   Do a quick search, and you'll find a number of certifications, or "trust me" seals, which you can post on your website. These verify that you're up-front about your use of visitors' personal information. While the European Interactive Digital Advertising Alliance, a cross-industry self-regulatory initiative, has perhaps the best-known program in the EU, it remains to be seen how effective programs like this one will be in gaining consumer trust worldwide.

2. **Clean up your current lists.**
   Make sure your subscriber lists are up to date. Consider getting rid of "dead weight" — names that have been on your list for a while and never generate any engagement. Start with a clean-ish slate.

3. **Stay up to date.**
   Privacy is a topic that is in flux, so follow thought leaders to stay informed. We recommend:

   - **Duncan Smith, a U.K.-based expert on compliance problems, data protection, and privacy audits: @Duncan_iCompli**
   - **Laura Atkins, an Email Strategy and Delivery Consultant, Word to the Wise: @wise_laura**
   - **Liz Smyth, Marketing Director, Marketo Europe: @lizsmyth**

4. **Raise the privacy bar in your organization.**
   Work on the business case. Demonstrate that you can affect sales by raising trust with your target audience. Make sure you understand how privacy affects people's behaviors in your particular business.

5. **Find out how your target audience feels about privacy.**
   Ask them directly. Get feedback on your current practices. Do some A/B testing.

6. **Use personal data to deliver demonstrable benefits.**
   Think back to the Amazon.com example. Such companies successfully gather enormous amounts of information about customers and use it to build successful relationships.

7. **Conduct privacy impact assessments.**
   Privacy by design — the ability of consumers to precisely dictate how you can track and use their data — is on its way. The sooner you start assessing your privacy practices, the better off you'll be.

Align Your Backend: 5 Simple Privacy Impact Assessments (PIAs)

PIAs are common-sense technical tweaks that will give you valuable information about your privacy practices and raise your confidence in the face of the changes we've talked about. Taking the initiative to sync your system with upcoming privacy regulations will also curb technical headaches later on.

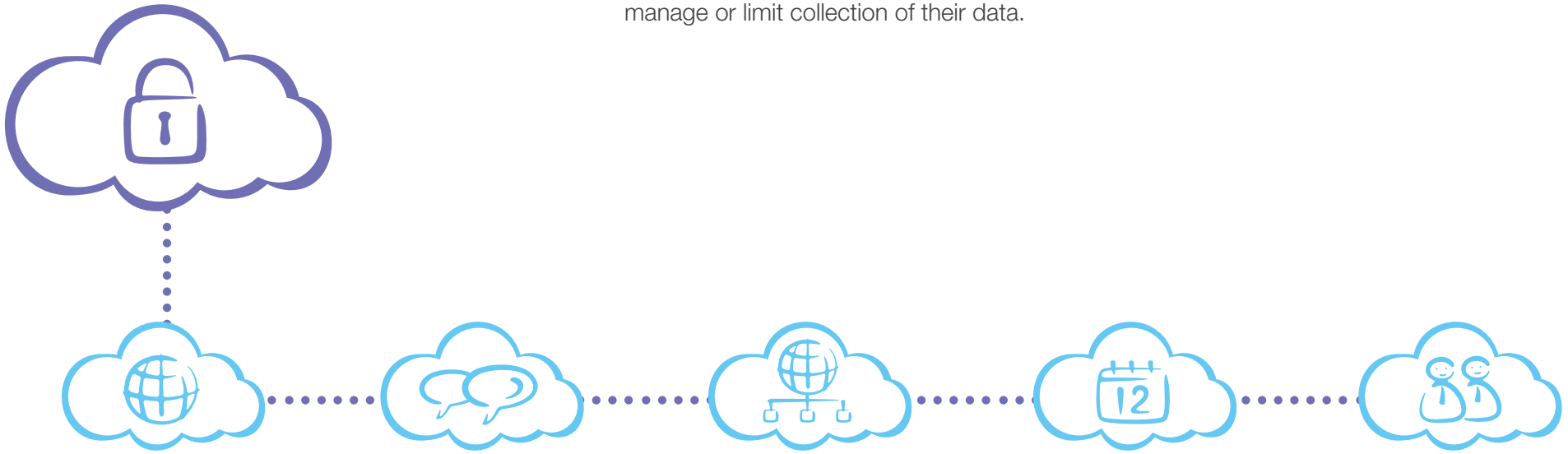
1. **Do an inventory of your websites.**
   Review your web assets and make a note of any pages that are dropping cookies or tags on your visitors' computers in order to personalize the information you are giving them.

2. **Tell people what you're doing.**
   Confirm that all those cookies or tags are detailed in your privacy policy so you aren't keeping secrets. Full disclosure builds trust.

3. **Give them choices.**
   Make sure that first-time web visitors receive a clear message that your site uses cookies. Tell them how to manage or limit collection of their data.

4. **Set your CRM system to include a provenance field.**
   Demonstrate to regulators and customers that each person in your database has given you their information for the purpose of marketing. The provenance field is where you record the date, time stamp, and origin of that data.

5. **Begin recording data provenance on all new contacts and leads.**
   Start now and you'll be well positioned for any challenge to your privacy practices.



The Calm After the Storm: When Customers Trust You, All is Well

It's easy to get overwhelmed by the various privacy changes happening around the world. But, as marketers, we must remember that we don't just sell things. We tell stories that inspire people to invest in our brands — and how we tell those stories is just as important as the stories themselves.

Getting on board with privacy regulations makes us imminently trustworthy with consumers. Let people decide for themselves how much information they want to give you, and how they want you to use it. Let your story be one of mutual trust and respect.



This eBook was written in collaboration with Duncan Smith, MD of iCompli®; a specialist consultancy delivering compliance solutions in the arena of information law, privacy and corporate social responsibility. iCompli® works closely with clients to implement practical, technology-led solutions to help deliver the lawful, ethical and profitable use of personal data.



Marketo (NASDAQ: MKTO) provides the leading marketing software for companies of all sizes to build and sustain engaging customer relationships. Spanning today's digital, social, mobile and offline channels, Marketo's® customer engagement platform powers a set of breakthrough applications to help marketers tackle all aspects of digital marketing from the planning and orchestration of marketing activities to the delivery of personalized interactions that can be optimized in real-time. Marketo's applications are known for their ease-of-use, and are complemented by the Marketing Nation™, a thriving network of more than 250 third-party solutions through our LaunchPoint™ ecosystem and over 40,000 marketers who share and learn from each other to grow their collective marketing expertise. The result for modern marketers is unprecedented agility and superior results. Headquartered in San Mateo, CA with offices in Europe, Australia and a joint-venture in Japan, Marketo serves as a strategic marketing partner to more than 3,000 large enterprises and fast-growing small companies across a wide variety of industries. For more information, visit **www.marketo.com.**

The materials on this website are provided for general informational and educational purposes only and do not constitue legal advice. They are not offered as and do not constitute legal advice or legal opinions. You should not act or rely on any information contained in this website without first weeking the advice of an attorney.

08042014