Marketing and Privacy in the Era of Data—Some Useful Tips for Playing it Cool

Behavioral ads, social tracking, data lakes—the pressure is on Marketing to perform faster using a plethora of often silo'd digital tools. It's challenging to find the time to pause and think beyond the push to target customers with ever-greater precision. But a little perspective and a few upfront steps can make a critical difference to protecting your company, your customers and possibly your career. From cyber breaches to data brokering, there's a lot of confusion about what's happening with our data. It's an issue of brand trust as much as liability. These tips will help marketers get the job done and better manage data risk:

Know what's promised—and not—in your company's privacy notice

Privacy notices – those external-facing documents that give customers the Ts & Cs of sharing their data with you – have become de facto for most businesses, and are often legally required. Even though these policies can be lengthy and challenging to read, they're a binding agreement with anyone whose data you collect. And there ARE people who read them! Know what your company notice says is being done with collected data – and make sure that actual practices align to that promise.

Match your product or service claims to reality

If you've ever written marketing copy, you know the irresistible urge to shout about how great your products or services are. Just be careful how you phrase the benefits. A little puffery is generally ok, but no one can truly 'ensure' that data security is 100% guaranteed or that your company's approach is absolutely the best practice or your product is entirely defect free. If you make such claims, someone just may hold you to them. Find clever ways to make value claims that still match what is truly possible. You'll need to run it by Legal anyway, so get a head start and wow them with your savvy messaging skills!

Understand what you're collecting and why you need it

It is so tempting to gather as much data as you can because "someday" it may come in handy. Data gets stale fast, limiting its useful shelf life. If you have a breach or some regulator comes poking around, you may well have to substantiate a business rationale for holding whatever data you possess. That means a real business purpose now, not a "maybe someday we'll use it" reason. You can't get in trouble with what you don't have, so gather what you truly need and let go the rest.

Don't be creepy!

Digital marketing can be highly targeted and personal but can also feel invasive. While marketing automation enables contact at more predictable times in the buy cycle, it can get overdone. People complain about ads following them for days after an online search, and ad blockers are growing in popularity. Increasing use of location tracking and facial recognition may increase a feel of stalking. Allowing opt out and always give users choice in how much information they receive how often. The Digital Advertising Alliance offers some helpful guidelines too.

If texting campaigns are part of your marketing mix…

Text messages to mobile devices are covered by the Telephone Consumer Protection Act and certain Federal Communications Commission rules. It's prohibited to send texts to mobile numbers without express consent from the owner of the number. This practice can end up with a fine to your business or even law suits, so be sure you have permission before hitting 'send'.

When your target market is kids

It's flat out against US law to collect personally identifiable information on children under age 13 without their parents' consent. That includes things like monitoring what sites they go to, what they look it, their social media practices and their location data. You need to get explicit parental permission, or this can get serious. Yes, actual proof of age can be a little tricky – but using online verification methods and showing good faith efforts will help keep you covered.

Doing business in Europe?

If your company collects information about EU citizens, there has been a very recent change to how that data needs to be treated. European laws around citizen privacy are far more strict than those in the US, and in 2016 they got even more so. You will need to adhere to a new initiative called the EU-US Privacy Shield. And in 2018, a major new law called the EU General Data Protection Regulation (GDPR) goes into effect – so start planning now. Oh and that marketing to kids thing? The GDPR raises the applicable age to 16! There are probably some royal battles coming with mom and dad over that one.

Mind Your Workspace

While malicious outsider cyber-attacks are real and increasing, the majority of data breaches are caused by human error. Accidental data exposure, lost devices, disgruntled workers doing bad things, papers laying around, unsecured computer screens…any of this ever happen in your workplace? Staying aware of what's available to whom can go a long way in keeping data secure.

Don't Know Where to Start? There are some good practices to follow that will help. For new ventures, integrate a practice called Privacy by Design from the get go. That means designing in the right way to handle data from the beginning. For operations already in place, a Privacy Impact Assessment will help you understand what's working well and what might need improvement. Such upfront efforts can help make the most of the data and tools you have while enabling an informed choice about how much risk your business should take.

Sounds a bit daunting? We feel your pain. With years of marketing expertise and current data privacy know-how, **DIALOG RESEARCH & COMMUNICATIONS** is ready to be your on-demand data privacy manager—for a little or a lot of help.