Brand Reputation in the Era of Data

8 Principles for Trustworthy Data Stewardship That Won't Kill Your Customer Relationships

DIALOG RESEARCH & COMMUNICATIONS

December 2015

An Introduction.

At what may be the dawn of a radical new era of technologically-driven marketing capability, I have been wondering – is enough ever going to be enough for the people being marketed to? People love their apps. They love online shopping. They love free stuff. They love connecting digitally to their friends and family 24×7. Even the growing stream of data breaches doesn't seem to have much behavior-changing effect.

But the game is accelerating. Predictive intent, always the brass ring of marketing, is becoming ever-more precise, thanks to unprecedented analytics capabilities, big data, and soon-to-be connected everything. We may be heading toward something like **on-demand lizard-brain manipulation**—with marketing suggesting what people are going to want to buy before they are consciously aware of it themselves—with greater and greater accuracy on the timing of when a desire will manifest. That's a future vision I don't think many people understand.

So I thought I'd pose a simple question. DIALOG recently conducted a study in which respondents were asked how they'd like marketers to behave in a predictive analytics world, mining data from the places the respondents digitally engage – willingly or not, knowingly or not. Respondents ranged in age from 30 to late 60s. They were male and female. They were all Americans, except for one subject of Her Majesty. Most have a college degree, a few have a Masters, and a few work (or worked) in marketing-related jobs. They all willingly and regularly participate in the digital economy. And they all sense a lack of control over data about themselves.

One of the things that most struck me was that **people have a general, vague awareness that 'they' are tracking everything about us**. But less clear is who 'they' are or what's being done with the data. Although I asked for gut reactions, what I got instead from the great majority were thoughtful, detailed and impassioned responses. Clearly this topic pushes a button. There is a growing undercurrent of discomfort. General discomfort will get quickly targeted toward any particular brand that pushes too far. Several respondents expressed (unprompted) anger at particular brands they felt disrespect their relationship. Given the huge investment required to build positive brand reputation, **active customer anger should be every marketer's (and CEO's) nightmare**.

The patterns that emerged from all of the respondents' feedback were clear. It's time to change some behaviors. While our sample population was small, the findings from our formal query are backed up by countless informal conversations, and reinforced a later report from the Pew Research Center[1], who conducted a similar study with 500+ responses. In the interest of something actionable, DIALOG offers this set of 8 Principles for Trustworthy Data Stewardship to help preserve customer good will and brand value. We request and welcome thoughts and feedback to further this important discussion.

[1] http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

Principle 1: Empower Customer Control

I know right off the bat that espousing customer control of coveted data collected at great effort and expense is marketing heresy. But it's what the respondents want. **Sensed loss of control** (psychological or otherwise) was the predominant finding in DIALOG'S recent research.

Control extends to multiple domains. Perhaps most contentious is **who 'owns' someone's data**. People believe they own their own data; the businesses who collect it feel they do, and in reality, they do legally own what's collected in the course of transacting business. Customer data is a critical asset. But what happens with that data beyond the original intent (a la "I know I bought a thing from you but not them") is unclear and uncomfortable. Some want access to their data to see what's been collected. Some feel that they should be paid for the use of it. Most want the option to decide whether or not their data gets shared, with whom, for what purpose and in what circumstance. This is far from today's practices.

The letter of the law may permit sharing or selling of data to 3rd parties. Long, complex privacy policies in 3-point font may direct customers to some limited opt-out actions. Those policies are SELDOM read and even less seldom understood. But perception is what really matters. **When customers feel loss of control over how their data is used and abused, offending brands will pay the price**. One respondent told me she could tell exactly which not-for-profit entity had been repeatedly selling her data by the volumes of spam received; she stopped supporting that not-for-profit all together.

Control over the digital experience is another concern. If the internet is about freedom, then people should be free to direct their online experience, and not have a search engine or a business decide what they see. People passionately hate pop-ups, and don't form favorable opinions of the unwanted brands that pop up. Turning them off imposes a burden on the user, and blocking all pop-ups may interfere with desired experiences on other sites. Much preferable would be **inviting users to allow some dynamic messaging when they are open to receiving it**.

In that same vein, customers want to choose the frequency of interaction. A positive purchase experience can easily sour by excessive promotional emailing. One respondent told me she regularly unsubscribes from chosen brands who spam her, and those brands fall off her consideration list. I myself have done this. Another respondent expressed anger over being "tricked" by a brand who slipped in a subtle clause on an e-commerce site that then obligated her to buy something she didn't realize and didn't want. In her words, this should have been opt-in, not opt-out. But she also told me she really appreciated that when receiving promotional material from a company she had not previously bought from, it clearly stated that she was receiving it because she had purchased from XYZ. That **transparency was enough to make her feel positive about the old *and* the new brands**.

THE INTERNET IS ABOUT FREEDOM. LET ME DECIDE WHAT I SEE

The marketing practices mentioned here are common. Industries are built on them. But as more data is collected from more connected 'stuff', these issues stand to multiply exponentially. It's not about what's legally allowed— it's about customer perception and experience. More empowered customer choice and control in the data relationship will bring rewards of stronger loyalty and brand reputation.

Principle 2: Be Clear and Accountable

How many times have you actually read the whole privacy notice of a vendor, financial institution, or app you put on a mobile device? Ever? The reality is that almost no one reads them. They're generally long, filled with legal jargon, and published in tiny, hard to read font. They all vary according to applicable law. They can be hard to find on web sites. The 'opt out' link is even harder to find.

Not reading them is no excuse for consumers who willingly enter a business relationship to claim ignorance or victimhood – or is it? When you accept a service, you are bound by the terms. But it is widely understood that privacy notices are very challenging for average people. There is a legal concept of **responsible use of personal data** that at least one legal expert I've heard speak says the US Congress knows is going to need to be legislated. Who knows when that will be?

It is safe to say that for now privacy notices are generally not working as they should. One of our respondents (a polished professional in a respectable job) reacted passionately with 'privacy policies stink!' as his gut opinion on this issue. So how can they be made better? And why should marketers even care?

YOUR PRIVACY NOTICE DOES NOT HAVE TO READ LIKE A DRY LEGAL BRIEF

The privacy notice presented to your customers is a legal covenant made with them. **It establishes a bond that is integral to your brand reputation**. But that doesn't mean it has to read like a dry legal brief. Done right, it should reflect your organization's values, attitude toward customers and interest in helping them understand terms of the business relationship – simply, clearly and transparently.

While privacy notices (also called statements and policies) must be developed and approved by those with legal and privacy expertise, Marketing has the communication expertise to simplify the language, put a customer advocate hat on, and **collaborate with the legal team to make this customer-facing document as clear and friendly as it can be**. Put it in words that read how people really talk. Make the mutual responsibilities clear and transparent. Spell out 'what this means for us', 'what this means for you', and what actionable options people have to empower control.

Make the notice readily accessible. Some of DIALOG's study respondents even suggested reminding them of the covenant every time they interact with a site or an app. Right up front. Plainly. And if a policy changes, what has changed should be immediately pointed out, allowing customers to opt out of the new terms on the spot. (By the way, changes should never be made retroactive. That's not legally permissible).

Then **consumers – read them!** As a few of DIALOG's respondents willingly owned, users have responsibility in this game. You get something for what you give up – money or information. But it's a choice. You can always choose not to use an app or a service. Last year, when Facebook spun off Messenger, I went to add it on my Smartphone to see a pending message. But then I read the notice of what I would be agreeing to in doing so – giving Facebook access to all of my non-Messenger text messages! (Why do they need that? How many of you saw that?) Almost all apps now do this. Most consumers do not even read these terms.

Beyond your external notice, make sure you have clear internal privacy policies. Then make sure everyone in your business is trained on them. Remind employees frequently to act with responsibility and accountability. And apply those policies consistently. Breaking the established customer bond is a quick way to kill trust and damage your brand. Clarity and accountability will strengthen it.

Principle 3: Do Everything You Can to Protect Customer Data

There are few hotter topics these days than cyber security. Sadly, the state of affairs will probably not significantly improve in the foreseeable future. Estimates are that two new malwares proliferate every second. Even the best intrusion protection software cannot keep up with that. The reality is that no organizations are infallible, and despite your best efforts, **you can and probably will get hacked**. The Ponemon Institute calculates the costs of lost business resulting from a data breach as having increased from an average of $1.33m in 2014 to $1.57m in 2015[2], with the cost per record increasing to $154, up 12% from 2014.

Still, organizations must proactively do everything they possibly can to protect customer data. With new breaches in the news (and notifications in our mailboxes) so frequently, people are rightly very concerned about the security of their data. Organizations who are thought to not have taken adequate security measures become the target of lawsuits. For example, Anthem is facing multiple suits after admitting a massive breach last February.

ORGANIZATIONS WHO ARE THOUGHT TO NOT HAVE TAKEN ADEQUATE SECURITY MEASURES BECOME THE TARGET OF LAWSUITS

While setting up digital protections is the realm of IT, there are **many other sources of risk to customer data** – such as employee negligence, being careless with physical documents, not securing file cabinets, not destroying data that is no longer needed, leaving unsecured computers accessible, malicious insiders and just plain old mistakes. An organizational culture of mindfulness about practices that may seem innocuous can go a long way toward keeping data secure. It's everyone's responsibility.

Our study respondents had **many other data protection concerns** as well: Hide my identity; Don't track (or reveal) my location – this is a particular concern for women who fear stalking; Don't use facial recognition to identify me in crowd scenes; Don't harm me or enable harm to me by sharing my data with others who discriminate or apply bias; Don't track health-related data and search queries; Don't share sensitive medical and financial information. Unfortunately, technologies are rapidly proliferating to do all of these things, and faster.

Just one example – at a conference in September 2015, I heard the Chief Privacy Officer for Acxiom say that their data analytics capabilities are advanced to where they can identify by name a large percentage of the US male population who were likely to have a certain health condition that, let's say, most would not want revealed. She had to call foul and was able to stop the general availability of these lists for purchase.
Clearly there are many facets to data concerns and data protection. Get your own house in order. Ingrain this into the culture. And be as transparent and reassuring as you can with your customers about how seriously your organization takes this. But then there's beyond your organization…

[2] Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, May 2015

Principle 4: Mind Your Partners!

While the last post discussed getting your own house in order around protecting customer data, equally important is **protection of that data when it is passed on to others in your value chain**.

Consumers regularly agree to share data with a particular organization for immediately known purposes – a purchase transaction, registering for a site or service, downloading an app. There is an abstract understanding that their data is shared. But the specifics of with whom, how and for what are vague to all but the most attentive, usually those who work in a marketing capacity. The New York Times estimated that the Acxiom, the country's leading data broker, will have about 1500 pieces of information[3] on an average individual! I didn't know there could be 1500 things about me to be tracked. Who knew I was so interesting? And then there's what the government collects…

This vague concept of 'they have all of my data' is unsettling, leaving people feeling powerless and *hoping* that nothing harmful will befall as a result. It is perhaps the greatest area of concern for our study respondents. Legal requirements are normally that **the data owner has bottom line responsibility** (read that the one who could be sued in a breach), so it behooves you as a data collector to integrate strict data management terms into your third party contracts.

1500 DATA POINTS TRACKED – WHO KNEW ANY OF US WERE SO INTERESTING…!

But beyond that, it's how the data is used and monetized – and we all know this is the holy grail of marketing – that respondents find troubling. One respondent noted that "3rd party access to my search history is completely inappropriate." Another noted that "if you got my data from somewhere else, tell me where you got it from." Some of the other concerns expressed included not allowing an individual's identity or data given for one perceived purpose to be used by entities that have control over other parts of their lives – insurance, credit, employers, housing, civil litigation, health care providers, surveillance or profiling, divorce court, political parties, or the news media, except as allowed by law. Data collectors should therefore carefully consider **legal requests vs. legal requirements**.

One respondent's suggestion was to have and observe universal standards on collection and distribution of sensitive and potentially harmful medical and financial information. There are already laws about these domains, but data analytics can get pretty accurate using other non-regulated data.

However, some respondents also took a Buyer Beware stance, saying that data voluntarily given and captured through public means is there for the taker, and consumers can always choose not to participate in a transaction. It is better to educate people about what is being harvested about them and how it is used so they exercise more informed choice. Agreed. Improving privacy policies would be a good start. But it can be challenging to get that message across when data is handed off to anonymous 3rd parties whose very existence or purposes are unknown to average people.

[3] http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0

With the Internet of Things, this situation will grow exponentially, creating further issues of securing data at the points of collection, transfer and curation x 1000 – and the implications for Big Data crunching that will come from it. Bottom line – mind your partners. Privacy protections need to be contractually obligated with third parties, but prudence dictates you avoid sharing with those who perpetrate the creep factor, especially when contributions can be traced back to you.

Principle 5: Practice Customer Empathy

Hand in hand with getting your house in order to secure customer data is developing an empathic **organizational culture** that understands, internalizes and practices customer-sensitive behaviors. This can be reflected in the marketing practices you adopt, the way customer data is collected and handled, and the attitude and values that are expressed and embodied from leadership through the ranks.

Several respondents in our qualitative feedback study emphasized that organizations' observing privacy policies internally was very important to them. While most every organization has an external privacy notice (understandable or not), many companies lack a robust internal privacy policy, data management policies, or even clarity of their privacy mission and position. It is important to thoughtfully define these, then **train your people, in a resonant and memorable way** about these corporate values and an employee's role in them. Reinforce the training with an ongoing internal awareness campaign. Help your team remember that behind every purchase, tweet, post, click and share is a human being and all that entails. Anyone who has something or someone to protect can understand that.

THOSE WHO DECLINE TO PARTICIPATE IN REDUCING RISK SHOULD BE MADE FULLY ACCOUNTABLE FOR THE CONSEQUENCES – FINANCIAL OR OTHERWISE

This is a foundational aspect of your organization's **personality and reputation** – how do you want to be seen and regarded? Are you the respectful company? The service-oriented company? One who customers see as sneaky or arrogant? One who is so consumed with innovation and speed that they forget there are real people who will be served or potentially harmed by your invention?

Consider incenting or requiring those who work with other's Personally Identifiable Information, whether it belongs to customers, employees, partners, students or anyone else, to **get certifications**. This can help them more deeply understand the implications of what they're working with. A colleague of mine likened this to how massage therapists are trained to respect the bodies of their customers, with their reputation and careers dependent upon following industry protocols.

A best practice is to conduct what's called a **Privacy Impact Assessment** (PIA) to evaluate risk in both existing and intended practices and services. This can be a detailed process, so some companies opt for a first-pass "threshold" assessment to see if the deeper dive is warranted. There are online resources to offer you guidance (Shameless commerce warning: DIALOG can help with these); you will need some understanding of the legal and regulatory environment in which you operate. Then, when you objectively understand the level of risk, you can consider adjustments to your practices or plans if necessary. Those who may decline to participate should be made fully accountable for any consequences – financial or otherwise.

Principle 6: Comply with All Applicable Laws and Regulations. Then Exceed Them.

There are a LOT of laws and regulations out there that govern data handling and privacy. They vary according to where you conduct business. The European Union has the strictest set of laws that are built on the principle of human rights. The United States has what's called a sectoral approach, that is different laws are set for different sectors – like HIPAA for health care, Gramm Leach Bliley for Finance, the Cable TV Privacy Act, the Electronic Communications Privacy Act and on. In the US, 47 of 50 States also currently have data breach notification laws, all of them slightly different. Asian countries adopt data protection laws and sectoral laws. Many Latin American countries have constitutional guarantees, data protection laws, and sectoral laws. Yikes! It's a lot to comply with – and just to keep things fun, laws and regulations are changing and updating all the time.

Realistically, marketers are not going to know every legal requirement that impacts their organization. But you should at least **be aware of the basic principles of what's allowed in the places you do business**, then coordinate with Legal (I know, I know!) on how to stay out of trouble. This discovery can also happen through a process called a Privacy Impact Assessment, mentioned in Principle 5.

Observing laws and regulations must be Standard Operating Procedure. But just **being compliant really isn't enough to enhance your position** in a fickle and frenetic market. Think about it this way – Do you want your child to just stay out of trouble at school, or be a leader in the classroom? Where's the attention going to go? You sure don't want to stand out in a bad way – like being one of the 256 app providers who violated the privacy terms they contracted with Apple.

THINK OF IT THIS WAY: DO YOU WANT YOUR CHILD TO JUST STAY OUT OF TROUBLE AT SCHOOL, OR BE A LEADER IN THE CLASSROOM?

Going beyond the legal minimum and making extra effort will help your business differentiate as a trusted source. Simplified privacy policy language will help. Minimizing data collection and retention (yes, you CAN get rid of stuff!) will help. So will being transparent at all times about your practices and behaviors. Use creative ways to tell the story to your customers and stakeholders – through vignettes, through messaging, through customer service scripts – put it out there! Earning trust marks like TRUSTe really sends the message that you take data stewardship seriously.

Your customers expect you to comply with the law. They want to feel like you care and are proactive about protecting their data. I firmly believe that the great majority of people want to do the right thing; it comes back to mindfulness and balance between enthusiastic pursuit of business objectives and a bit of thoughtful restraint.

Principle 7: Apply Technology Thoughtfully

In October, Chapman University published the results of its survey America's Top Fears 2015. Respondents were asked their fear level about different factors ranging from crime to disasters to their personal futures. FIVE OF THE TOP TEN THINGS PEOPLE FEAR ARE RELATED TO MIS-USE OF THEIR DATA!! That includes cyber-terrorism, corporate tracking of personal information, government tracking of personal information, identity theft and credit card fraud. That's out of 88 possible things to be afraid of!

There is a tidal wave of automation being applied to data collection and usage practices. I suggest that just because you can do something doesn't always mean you should. We are approaching a tipping point around the creep factor of having everything that one does be tracked. People are tired of constant advertisements, witnessed by the increased adoption of ad blocking technology, and especially Apple's recent iOS 9's robust blocking capability for Safari – which has been heralded as the potential death of online advertising. As ads are blocked, marketers need to find other ways to get their message through, such as direct contact with mobile devices. That will require permission from each user. And that means you have to be delivering a lot of value while also showing some restraint in the level and frequency of contact.

Another interesting wrinkle is the October 6 2015 ruling by the EU Court of Justice that struck down what is called Safe Harbor, a policy that allowed self-certification by US companies to say their data protection standards were sufficient for EU citizens, who are protected by strict privacy law. Israel followed suit on October 20. What happens next is yet to be determined, but everyone is scrambling to figure out how to protect their international business by the end of January grace period.

WE ARE APPROACHING A TIPPING POINT AROUND THE TRACKING CREEP FACTOR

When practices get abused, people fight back or tune out. It's human nature. In e-chatting during a recent webinar with its moderator Chris Surdak, a big data expert, (who I thought advocated for unbridled capitalism more extremely than anyone I have ever heard), he noted regarding privacy that **"The backlash will be epic, if we ever get there."** Hmmm. A thoughtful approach to what you collect, how you collect and use it, how long you keep what you collect, with whom you share it and what they do with it will better serve and protect your business and your brand through changes in customer sentiment and the regulatory environment.

Principle 8: Actively Demonstrate Respect for Your Customers

The final Principle clarifies a concept implied across the other seven. To become and remain a successful brand, businesses must actively demonstrate customer respect. Just saying 'We respect our customers!' is not enough. **Prove it**.

This can take many forms, from being transparent and honest about data collection and sharing practices to moderating your outreach below the annoyance level to integrating this attitude into your culture and policies – and many other opportunities mentioned through these pages.

NORDSTROM FIGURED THIS OUT A LONG TIME AGO

Disrespectful practices were often brought up in the comments I've gotten. One respondent noted that "I want to feel like a vendor respects my data as much as I do." People do not like bait-and-switch, confusing changes to privacy policies or anything that feels sneaky. They don't like the burden of responsibility to stop something, like too much email or too many pop-ups. When everyone is tired or busy from their own lives, wearing people down or hoping they won't notice **might produce a short term win, but not long-term loyalty**.

Having a straightforward dialog with your customers – even the ones who are unhappy with you – is another way to show respect. Everyone messes up – own it! Apologize, make it right and move on. If it wasn't your fault, but there's a small cost to making someone feel respected anyway – do it! Nordstrom figured this out a long time ago.

Nothing about customers wanting to feel respected and treated fairly is new. What is new is the exponential increase in vendor relationships enabled through technology. With the tremendous choice the modern customer enjoys, **utility, benefit, quality and value are now table stakes**. A differentiated and trusted experience, that includes feeling respected, is what will stand out. **Someone's choice of your product or service is a privilege**. One of the best quotes from the respondent feedback sums it up: "Respect the customer and the customer will respect you."

Should You Really Do It?

These 8 Principles will help marketers protect and strengthen their brands in an era of radical change, where there is great temptation (and quite likely management pressure) to push boundaries further than ever before. Throughout recent months, I've had countless conversations with people about the state of their data as well as the modern conveniences upon which they've come to rely. I've heard a Big Data expert actively advocating for stretching the law (or hinting at crossing the line) for the sake of competitive advantage. I'm sure he is not alone in that opinion. We are, all of us, currently in the Wild West.

While technology is accelerating what's possible, the ideas outlined in the 8 Principles come back to common fundamental and timeless human needs that will outlast every wave of technology: **People protecting what's theirs, seeking respect and dignity, wanting control of their lives, enjoying freedom and avoiding harm**. The brands they will choose for anything more than a one-time experience will be those who understand those concerns, and actively work to enable them.

There is more to brand reputation than being the app of the moment. Not every new thing will be transformational. But businesses who innovate as well as who truly respect their customers and actively work to earn trust stand a far greater chance of longevity than those who rely on buzz about the shiny new object, or who exploit to maximum advantage thinking the 'sheeple' won't notice. It will take work. It will take awareness. It will take intention. It will take courage. And it will take leadership.

Eventually today's Wild West will give way to a more mature market dynamic. Embracing these 8 Principles may help ensure your company is there when that time comes – or even leading the way. For now, this is an open and ongoing discussion. Your point of view is welcomed through any of the contact methods below. Thank you!

About DIALOG RESEARCH & COMMUNICATIONS

DIALOG RESEARCH & COMMUNICATIONS, a Small Woman-Owned Business, offers fast, insightful situation assessment, research, practical recommendations, and just-get-it-done execution needed to keep your organization on track during growth or transition. Services include:

- Research & Analysis
- Stakeholder Assessment & Mapping
- Strategic Communications Planning
- Key Messaging and Content Development
- Thought Leadership
- Program Management
- Data Privacy Risk Management

Contact: +1 925-719-1260
kstershic@dialogrc.com
www.dialogrc.com
@kstershic

