Chapter 1 - Data Reimagined

Trust is Powerful

Justin and I (but mostly I) are longtime customers of a national home goods store which, for the purposes of this book, we'll call Box and Keg. We got our first sofa there, stocked our cabinets with their mugs, and shopped there for our first child's crib and changing table. Our youngest is now a pre-tween, and B&K is still advertising nursery furniture to me. I am very much not in the market for crib sheets and adorable mobiles, but I don't want to unsubscribe from their mailing list because I see real value in the occasional email they send about the new trends in tween room decoration.

If they asked for the ages of my kids, I'd happily share that information with them because I like and trust the company, but every time they miss the mark, I'm reminded of how impersonal our relationship is. Box and Keg knows when I bought my first nursery item, so it could reasonably deduce I now have a child over the age of five. If it tracked that information and used it thoughtfully, it would stop sending ads for infant gear to me and age up what they showed me along with my kids. This would be an excellent use of data—to deliver better, more appropriately targeted messaging—and it would probably generate an additional sale or two for them.

Recently, another company that we'll call Globe Shop started sending me advertising. In one email, they even asked for exactly the information I'd wished Box and Keg had! But, because I've never shopped there and assume they simply bought my information from my credit card company, I went out of my way to unsubscribe from their list. Globe Shop hadn't yet earned my trust and was asking for data it didn't deserve. Box and Keg has my trust and isn't asking for data I'd happily share.

Companies that successfully reimagine data as a medium for strengthening their relationship with customers will first earn our trust and then ask the right questions to encourage us to willingly share more of our data with them. These organizations will then safeguard that data, use it for our benefit, and be transparent about that use, deepening their customer relationships by delivering tailored messages that create value for us—and a powerful competitive advantage for them.

Privacy and security experts who don't have an eye on the needs of businesses often make blanket statements condemning data collection, but that's not our argument. We believe in the promise of data and that companies should be collecting and using it to personalize their messaging. That said, we're also keenly aware of the dangers to which companies unwittingly expose themselves when they don't handle that data responsibly and with respect for the consumer. When they do, it can deliver additional competitive advantage by keeping companies ahead of (rather than scrambling to catch up with) both increasing legal regulation and customers' changing sensitivity to issues of privacy and security.

The Promise of Data

In the “real” world, when we walk into a store, even a local corner coffee shop, we don’t expect the barista (who may know our name and usual order) to know how much we make a year, the ages of our children and whether we’re in the market for a new car or a Mediterranean vacation. We made a human connection with a human representative of the company.

The online shopping experience is weirdly both less and more personal. Even relatively small e-commerce sites “know” a great deal about us. Technology enables companies to capture a tremendous amount of information, keep it indefinitely, connect it, and share it with hundreds of other companies in the name of connecting us all. Companies use that technology to the fullest, collecting every possible data point whenever and wherever they can, not because they have a clear business need for it, but because they’re not sure they’ll get another chance. In the rush to gobble up customer data, they forget the customer isn’t just data. We’re people. Data doesn’t shop for swimsuits and sunscreen. People do.

Justin: I’m hearing a theme here.
Jodi: I hear Italy is nice.

Having information about your customers isn’t the same thing as having a relationship with them. In fact, it can often have the opposite result. People are increasingly alienated and, to introduce a technical term—creeped out—by how much Facebook and Google “know” about us. If I’ve spent an hour online researching sunny islands, an unsolicited email from Air Malta doesn’t make the airline feel like my friend. It’s assuming a level of intimacy it hasn’t earned. In Googling for information, I’m doing the equivalent of looking at the work a local artist has hanging on the wall of my coffee shop. I do not expect him to show up at my house with a painting.

We believe consumers are yearning for personalized interaction with companies they can believe actually care about them. This is the promise of data that’s been appropriately used and respectfully handled. It can give your company the ability to provide unique, individually-tailored experiences that demonstrate to your customers in the respectful and transparent way you collect their data with their permission, use it to personalize your interactions with them, and protect it from misuse by others.

To users, data is personal. Gradually sharing personal information with one another is how human beings build relationships. Intimacy is a function of disclosure. We open up to people as we feel closer to them and close ourselves off when trust breaks down. The inverse is also true. We feel closer when we share information about ourselves and erode trust when we start to withhold information. Companies that collect consumer data without permission are effectively stealing the currency of intimacy, creating resentment rather than relationships.

The Danger of Data

Companies aren't wrong about the role data can play in building online relationships. In fact, what they often need is more data to do so effectively. The issue isn't the amount, but the way in which it's collected, stored, shared, aggregated, and used. When users trust companies the way I trust Box and Keg, they'll willingly share additional data. But trust must come first. Building privacy and security into the technology, not as an afterthought, but as an integral part of its design is the only way to create that level of trust.

Companies invest hundreds of thousands if not millions of dollars in cultivating and growing their brand to foster goodwill in their customers oblivious to the resentment they may be feeding just as aggressively. Worse, many risk the outright rage directed at companies when their lax security exposes their customer's data to hackers and thieves. Failures to treat people's data with respect can destroy in an afternoon all the goodwill and brand equity a company has spent years building.

People want to do business with companies they trust and feel good about. We want to like the companies we buy from. People love to buy from companies like Toms and Bombas because, for every pair of shoes or socks you buy, the company gives a pair away to people in need. In other words, people buy from them because they like the company. Failing to treat your customers' data with respect is a great way to make them not like you.

It's also beginning to cost companies business opportunities. People in B2B businesses think because they don't sell to consumers, privacy issues aren't relevant to them, but they are. I've seen deals not get closed because the company on the other side of the negotiation was concerned with protecting its users. As an example, in a common scenario, a company is shopping for a survey vendor. Being interested in building trust with customers and knowing that some survey companies aggregate survey data from their client companies and sell it, they want to know that won't happen. Those companies that can guarantee that have a competitive advantage. The same is true for security where companies are increasingly asking more probing questions and for audits and certifications of vendor companies.

B2C companies, on the other hand, are beginning to feel some pressure from consumers. A 2020 Pew survey showed that 52 percent of people would not buy a product or service over 1 privacy and security concerns. A few companies are beginning to look at the ethical questions raised by data collection, use, and storage as part of their ESG initiatives. They're recognizing, on a purely pragmatic level, that how they handle customers' data says something about their ethical standards and who they are as a brand. For most companies, these concerns aren't yet pressing enough to drive behavior change. Of the few who are paying attention, some are starting to recognize exciting opportunities.

Another Competitive Advantage

We have a friend who is a few years older than we are and has happy memories of family road trips taken in an old, wood-paneled station wagon. The car's "way back" had facing seats and she and her sister would alternately play on the floor and hang the top half of their bodies out of the roll-down rear window. She's not sure the car even had seatbelts.

Today, when she gets in her designed-for-safety, airbag-equipped, crumble-zoned car, she pulls on her over-the-shoulder-and-across-the-hips seatbelt without consciously processing it. This is the level of seismic mindset shift that's headed our way. And for much the same reasons.

While a few car companies were advertising safety features before Ralph Nadar's Unsafe at Any Speed, most weren't terribly interested in how their vehicles performed in a crash. They marketed their cars' shiny new features, performance, and speed. It was only after Senate hearings prompted by Nadar's book resulted in the formation of the federal Department of Transportation that seatbelts became mandated equipment in 1968.

When Mothers Against Drunk Driving started educating the public about their life-saving power, more people started to actually use them, but the first state law requiring drivers and front-seat passengers to wear them wasn't passed until 1984. By the end of the 1990s, over 60 percent of states had passed seatbelt laws. Today, New Hampshire is the only state that doesn't require them for drivers over eighteen. The laws vary widely, state by state, but usage was estimated to be an impressive 90.3 percent in 2020.

Today's internet is where the US auto industry was in the early sixties, and data privacy and cybersecurity are the seatbelts most companies aren't that interested in. Businesses today as then (as always) are profits-driven, and there's not an obvious bottom-line business case for safety measures until they're enforced industry-wide. This is an enormous opportunity.

When in 1990, with European car companies' sales in steep decline, Volvo's went the opposite direction. The company credited its longstanding (and at the time, somewhat aberrant) practice of advertising its cars' safety features. Volvo was associated in consumers' minds with safety before they started prioritizing it and while Oldsmobile was still actively and vocally fighting against regulatory legislation.

In this little parable, Apple is Volvo and Facebook is Oldsmobile. Facebook has consistently and repeatedly chosen to prioritize advertisers and its own algorithm over its users' privacy. Apple, on the other hand, has been garnering goodwill, recognizing the very real opportunity to engage their customers around something people are starting to care more about. Many other companies, especially small ones, have been practicing an "Ignore it and hope it goes away" policy, but this is changing.

The first US data breach law was enacted by California in 2002 and went into effect the next year. Today, there are fifty-two such laws (one for each state and two US territories). In 2004, California again led the way with the CALOPPA (California Online Privacy Protection Act which required websites to carry privacy notices, and a few other states followed suit. In the following years, there have been a flurry of new laws (which we'll discuss in more detail a little later).

In 2021, in the wake of the Colonial Pipeline ransomware attack, the federal government started getting serious about cybersecurity. Companies are already required to deal with all existing

regulations, and more are on the way. The lawless “Wild West” days of doing business on the internet are coming to an end and companies that get ahead of the new laws will enjoy a significant competitive advantage.

To do that, they’ll need to start attending more carefully to how they collect and use data (privacy) and how they prevent unauthorized access to it (security).

Data Privacy and Security Differentiated

While we’re sure there’s an analogy to be made to our marriage, the easiest way to explain the relationship between data privacy and security is to think about it like your house. If you have an alarm system, three locks on every door, and bars on the windows, your house is probably fairly secure. You’ve made it as hard as possible for bad people to break in and steal your stuff or hurt your family. But if anyone can peer in from the street because you leave the curtains open, your house isn’t private.

And maybe that’s okay with you. It’s just the living room, right? You probably don’t have a street-facing plate glass window in your bathroom. If you do, I bet it’s high in the wall or kept curtained. Likewise, you probably don’t mind having your first and last name and photo on LinkedIn, but you probably strip your street address and phone number out of your online resume and don’t include your height, weight, and last blood pressure reading.

Your doctor’s office, on the other hand, does have that information about you on its computer and if it’s properly set up, the medical staff has access to it, but the receptionists do not. They’re probably lovely people, they’d never break into your house, but they’re not authorized to look at your medical information, and making sure they can’t inadvertently access it is a security concern. To return to our house analogy, if you host a block party and move your prescription meds to the upstairs bathroom you’re hoping for privacy. If you lock them in a drawer to make sure nobody sees (or steals) them, you’ve secured them.

The distinction can get subtle. If someone uses your upstairs bathroom during the party and reads all the pill bottle labels, it’s a breach of privacy. If they steal a pill or two—from the medicine cabinet or the locked drawer—you’ve had a security breach. To use a more business-relevant example, if you walk into REI and buy a ski jacket with your credit card and then get flooded with brochures from Telluride and Breckenridge because REI connected your credit card data with your email address and sold that combination of information (that this person at that email address bought this coat) REI has violated your privacy. Their security people may well have done their jobs if the databases that hold all your information are adequately protected and don’t get hacked, but the company has still jeopardized consumer trust. Although what they’ve done isn’t necessarily illegal (depending on their initial disclosure), it’s a violation of our expectations.

Chapter Summary

Companies that can reimagine data as the new medium of trust decide to proactively care about privacy and security, recognizing the promise it holds out to build trust and demonstrate respect for their customers. They make it part of their sales pitch to other businesses and consumers alike, and get ahead of changing legislation, avoiding the costs in time and money of trying to retrofit their operations.

Now, more than ever before, business relationships (like all relationships) are built on trust. Trust has never been easy, but the ubiquity of data and rapidly changing technology—the very things that make it more e important—also make it more difficult. Here again, the answer is to reimagine data.

[1]https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-productor-service-because-of-privacy-concerns/