www.pipelinepub.com
Volume 18, Issue 5

Protection Over Profit: The New Consumer Data Paradigm

By: Ryan Jaeger

Historically, societal standards mandate asking permission before intruding and invading privacy. Strangers and friends alike knock before entering the sanctuary of our homes. We can choose whether we answer our phones, listen to voicemail messages, or return calls. We can unlock driveway gates only for those we know, trust or who approach by invitation.

These are long accepted as courteous privacy protocols. Yet, there is a marked disconnect between those societal protocols and what is currently practiced by many technology and e-commerce companies and applications regarding personal habits in our online spaces: exploiting data about those habits and actions. It's a disconnect that most consumers appear to accept by the tacit agreements required to use these "free" applications and services. But are consumers aware of how their data is being used?

Enterprises argue that they provide adequate data use notifications, and that their customers have "opt-out options." But these arguments leave several unanswered questions:

- How transparent are enterprises in how they use customer data for profit and more importantly, in how that data can be used to the customers' detriment?
- How easy is it for customers to find and then execute their opt-out options?
- Are customers fully aware of how companies are profiting from their data?

And finally, why should this customer data continue to be more vulnerable than consumer credit or health record data?

Leaving these questions unanswered—or adroitly avoiding or redirecting them—and not demanding enterprise accountability for customer data protection and use are most certainly antithetical to providing an optimum customer experience.

The credit data protection standard

Perhaps consumers believe that security and privacy protocols are commonplace among technology companies and mobile app developers who "serve" them. Perhaps their seemingly resigned complicity in agreeing that their individual data can be collected stems from an assumption that most if not all companies act similarly to those that check credit reports: the data cannot legally be used for anything other than what the consumer has agreed to.

Whether consumers actually believe they have legal data protections, or are operating within a veil of complacency, nothing could be further from the truth when it comes to consumer data protections. Unlike federal laws protecting credit data, or Europe's General Data Protection Regulation (GDPR), U.S. customers have only a patchwork of federal laws applying bandages to a festering privacy wound. A few states—namely California and New York (for financial services companies)—have taken the matter of data protection regulations into their own hands, but so far, the other 48 have not found enough legislative consensus to follow suit.

To be sure, consumer advocacy was not the primary driver in our country's earliest days of "credit reporting." Rather, companies were trying to make better lending decisions by attempting to filter out personal rumors and misinformation from consumers' financial integrity, a process that did not entirely leave out highly personal consumer matters.

Privacy concerns greatly increased as credit reporting records became computerized—so much so, that in what would unknowingly become a 20th century foreshadowing event, Congress held hearings to learn about such concerns.

The difference, in what perhaps is a needle of big tech's influence over the last half century, is that those hearings led to a change in federal law with the enactment of The Fair Credit Reporting Act (FCRA) in 1970, a piece of legislation that would evolve with increasing credit data concerns.

Congress sought to legislatively fix a significant problem in how consumer credit data is used. Why, then, is personal online customer data now so subordinate to credit data when it comes to protections?

The data revenue "model"

The truth about how companies are collecting and using customer data is not a pretty one when we lift the cloak of "customer experience optimization" to reveal the true motivation: *profit*. Enterprises are selling this data to generate revenue and doing so without customer—or even regulatory—transparency.

Did the average consumer agree to this?

Better put, as this quote from a privacy company executive somberly articulates in this 2018 PCMag article:

"If a company came to you and said, 'Fill in this form with all your personal information because we can sell it for $39,' no rational person would agree to it."

The top data profiteers are, not surprisingly, some of the largest names in tech: Google/Alphabet, Facebook/Meta, Twitter and Amazon are currently large revenue generators from user data. But other companies that hold data may also be poised to benefit from their customers who "agree" to share data, without explicitly understanding that those (and other) companies can then profit from that data.

Genetic testing companies offer one example, with some holding a repository of customer genetic data that can then be used for what could admittedly be valuable pharmaceutical research. It still, however, follows a pattern of asking customers to share private information for corporate profit without financially compensating customers who have already paid for a service. Why not pay them for their data?

It also leads to other concerns. First, genetic data is not individual—it's shared by perhaps thousands of family members—yet only one has to consent to having their lineage data shared and sold. Second, this genetic data sharing is surprisingly *not* covered under our country's HIPAA Privacy Rule, once again leaving states scrambling to catch up to deepening privacy crevices.

Microsoft and Apple also collect consumer data, but both have enjoyed a (deserved) reputation of being fastidious in their customer privacy policies and practices. Apple's privacy emphasis was publicly tested in its famous 2015 tussle with the FBI over creating a "back door" that would allow the FBI to unlock data from the phone of a suspected killer. In fact, one of its most recent changes directly targets how Facebook tracks and uses consumer data, putting it at odds with the "mega" Meta social media giant.

Still, that didn't stop Italy from levying fines against Apple and Google recently, claiming that Apple somehow conditions its customers into accepting its terms—while slamming Google for making it difficult for users to opt out of their consent for data collection and use. (Both companies are appealing the fines.). It's yet another sign of other countries holding enterprises accountable in securing customer data.

Notable, too, is that the two mega-tech enterprises with the best reputation for protecting consumer privacy as part of the ultimate customer experience—Apple and Microsoft—do not rely on revenue generated by their use of customer data as their business model. And that's key.

What enterprise experience are customers actually getting?

Even if savvy customers pay close attention to data collection notices, they may not always be aware of how that data is *used*, or that it is being sold for corporate profit. Some companies that

provide free social media interactions or search engines argue that it's a small price to pay for consumers to get their free services.

If customers, however, realized that their data is sold to a third party, which can then sell that data repeatedly, would they consider that to be a fair "price" to pay for likes and shares? Would customers agree to this "price" if they realized that data detailing their purchases of red meat or potato chips were sent to insurance companies, who used it to justify raising their premiums? Would Facebook users agree that the behemoth site has a right to "own" their Advertiser ID—a footprint that tracks not just customer purchases, but also where they go and even who they visit?

It's not just "free" social media sites. Some subscription-based sites track what consumers regularly purchase, then mark up the prices on those items because they know another purchase is likely. Data broker sites, like Spokeo and Whitepages, even require users to pay a fee to view the complete "data dossier" they have on a consumer. They compile the data from public sources, some of which may be unknown to the consumer. Then the consumer is asked to pay for it for company profit.

We should be focused on driving an environment centered on **full transparency** and **active participation,** one where consumers can easily (and freely) access, understand and know with certainty how and when their data is being used. And this should be happening across all industries and sectors, whether a company serves consumers directly or partners with other businesses that utilize consumer data as a part of their platform's experience.

At Flueid for example, our SaaS platform uses traditional and nontraditional data sources to help our clients make decisions and streamline the real estate transaction process from end-to-end. We intentionally designed data security at the core of our architecture and instituted processes and protocols to facilitate the use of data in accordance with its intended and permissible purpose.

We also don't store or aggregate any data within our system and encrypt every transaction placed through our platform at the individual order level. This means that data stays with the Flueid client, inaccessible to anyone else or other clients, for any other purpose—giving the customer the secure and private experience they have a right to expect.

Where do enterprises go from here?

Many enterprise customers likely do believe their data is protected—until it's not. Year over year, millions of consumers are snared in data breaches, and 2021 set a new record with almost 50 million victims. We've learned, as enterprise executives, that we can make security breaches more difficult, and we can mitigate their impacts, but we can't entirely eliminate them. However, allowing consumer data to be collected without optimum barriers surrounding that data, and then sold multiple times without the customer's knowledge, repeatedly exposes that customer's data in places that catch the customer unaware when a breach happens This is ultimately

because the customer never knowingly agreed to let their data travel to such places in the first place. Or at least, their opt-in was vague and confusing enough that they signed that right away.

Providing the optimum customer experience requires us to do better. It's our shared responsibility to ensure data protection, regardless of the extent to which data is used within a platform. We need to put more secure barriers around the customer data we collect; submit to regular audits to gain SOC 2 Type 2 certification to gain and keep customers' trust; and automate security checklists to reduce human involvement, thus minimizing human error. We must adopt a business model of transparency in how you use—and protect—your customer data in a format that is plain and easy to understand.

In other words, it's essential to put barriers around your customers' lives that prevent anyone from going into the inner sanctum of their daily lives, including you, without their permission.

There will be a day, and it's likely coming soon, that customers are going to value enterprise transparency and customer *empowerment* more than "optimization" as key to their overall customer experience. They will demand to not just *know* where their data goes, but also to have a say in their data end game.

If we as enterprises don't hold ourselves to higher standards, if we don't agree to industry benchmarks when it comes to protecting not just customer data, but also our customer's *rights* to that protection and privacy, we will ultimately find ourselves bound by legislation that denies us opportunities to grant the ultimate customer experience by our own business criteria.

Instead of finding ourselves knocking on customers' doors with no one answering, let's all—enterprises, technology, e-commerce companies, and app developers alike—do our part in protecting consumer data. We *can* innovate without imposing a weight of solicitation and secrecy on the backs of our customers.