Harvard
Business
Review

Data Management

The New Rules of Data Privacy

by Hossein Rahnama and Alex "Sandy" Pentland

February 25, 2022

WaffOzzy/Getty Images

Summary. After two decades of data management being a wild west, consumer mistrust, government action, and competition for customers are bringing in a new era. Firms that generate any value from personal data will need to change the way they acquire it, share it,... **more**

The data harvested from our personal devices, along with our trail of electronic transactions and data from other sources, now provides the foundation for some of the world's largest companies. Personal data also the wellspring for millions of small businesses and countless startups, which turn it into customer

insights, market predictions, and personalized digital services. For the past two decades, the commercial use of personal data has grown in wild-west fashion. But now, because of consumer mistrust, government action, and competition for customers, those days are quickly coming to an end.

For most of its existence, the data economy was structured around a "digital curtain" designed to obscure the industry's practices from lawmakers and the public. Data was considered company property and a proprietary secret, even though the data originated from customers' private behavior. That curtain has since been lifted and a convergence of consumer, government, and market forces are now giving users more control over the data they generate. Instead of serving as a resource that can be freely harvested, countries in every region of the world have begun to treat personal data as an asset owned by individuals and held in trust by firms.

This will be a far better organizing principle for the data economy. Giving individuals more control has the potential to curtail the sector's worst excesses while generating a new wave of customer-driven innovation, as customers begin to express what sort of personalization and opportunity they want their data to enable. And while Adtech firms in particular will be hardest hit, any firm with substantial troves of customer data will have to make sweeping changes to its practices, particularly large firms such as financial institutions, healthcare firms, utilities, and major manufacturers and retailers.

Leading firms are already adapting to the new reality as it unfolds. The key to this transition — based upon our research on data and trust, and our experience working on this issue with a wide variety of firms — is for companies to reorganize their data operations around the new fundamental rules of consent, insight, and flow.

Converging Forces

We see three distinct pressures currently driving change in the personal data industry. All three are quickly becoming widespread and intertwined, causing seismic ripples across the sector.

1. Consumer mistrust. The idea of "surveillance capitalism," which its author Shoshana Zuboff describes as "an economic system built on the secret extraction and manipulation of human data," has become common coinage, capturing consumers' increasing awareness that their data is bought, sold, and used without their consent — and their growing reluctance to put up with it. People are starting to vote with their thumbs: in the core North American market, both Facebook and Twitter are facing declines in their daily active users.

2. Government action. Federal lawmakers are moving to curtail the power of big tech. Meanwhile, in 2021 state legislatures proposed or passed at least 27 online privacy bills, regulating data markets and protecting personal digital rights. Lawmakers from California to China are implementing legislation that mirrors Europe's GDPR, while the EU itself has turned its attention to regulating the use of AI. Where once companies were always ahead of regulators, now they struggle to keep up with compliance requirements across multiple jurisdictions.

3. Market competition. Last year, Apple's upgrade to its iPhone operating system allowed users to shut down data harvesters' ability to track them across their many apps. It was a refreshing change, providing customers with power and agency over their data. It also bit hard into companies that rely on cross-app tracking: it cost the major social media sites $10 billion in lost revenue in the second half of 2021. Facebook's parent company, Meta, expects it will cost another $10 billion to them alone in 2022. Apple has made privacy protection a market differentiator: device manufacturers and app developers now use privacy features to draw new users.

This is a remarkable confluence of forces, and they are converging towards a clear endpoint where individuals will soon exercise full control over their personal data. While consumers still seek the conveniences and benefits that flow from their data, they will be the ones to set the terms over what data they share and who they share it with. People want that protection, governments have their backs, and technology firms are already falling in line, with competition over data privacy now impacting financial bottom lines.

Challenges Ahead for Large Firms

For established companies, these changes present a new set of data challenges on top of the ones they already have. Most large firms already suffer from a series of internal tensions over customer data. They typically have a Chief Information Officer whose role is to keep data in: collect it, encrypt it, and secure it from hackers. They also have a Chief Digital Officer whose role is to push data out: mine it, model it, and use it to entice users. Some have also added Chief Data Officers — a notably unstable position due, unsurprisingly, to lack of definition for the job — as well as Chief Information Security Officers and Chief Privacy Officers.

All these overlapping roles are embedded in organizations with expansive data collection operations, multiple legacy systems, a complex web of bilateral and multilateral data-sharing agreements and, quite often, an ongoing lack of clarity on how to integrate data into their businesses. Based on our experience, up to 90 percent of current IT budgets are spent simply trying to manage internal complexities, with precious little money actually spent on data innovation that improves either productivity or the customer experience.

The new data economy won't tolerate this state of affairs for long. If your organization generates any value from personal data, you will need to change the way you acquire it, share it, protect it and

profit from it.

The New Rules of Data

Our new rules of the data economy are fairly straightforward, all of them derived from the basic principle that personal data is an asset held by the people who generate it. But each rule entails the breaking of entrenched habits, routines and networks.

Rule 1: Trust over transactions. This first rule is all about consent. Until now, companies have been gathering as much data as possible on their current and prospective customers' preferences, habits, and identities, transaction by transaction — often without customers understanding what is happening. But with the shift towards customer control, data collected with *meaningful* consent will soon be the most valuable data of all, because that's the only data companies will be permitted to act upon.

Firms need to consistently cultivate trust with customers, explaining in common-sense terms how their data is being used and what's in it for them. Firms can follow the lead of recently-created data cooperatives, which provide users with different options for data sharing and secure each user's consent for the option they are most comfortable with. The more robust and thorough your consent practices are, the more valuable your customer database becomes.

Rule 2: Insight over identity. Firms need to re-think not only how they acquire data from their customers but from each other as well. Currently, companies routinely transfer large amounts of personal identifiable information (PII) through a complex web of data agreements, compromising both privacy and security. But today's technology — particularly federated learning and trust networks — makes it possible to acquire insight from data without acquiring or transferring the data itself. The co-design of algorithms and data can facilitate the process of insight extraction by structuring each to better meet the needs of the other. As a

result, rather than moving data around, the algorithms exchange non-identifying statistics instead.

For instance, many of Google's apps, such as the Swipe typing facility, improve phone performance by analyzing customer data directly on their mobile phones in order to extract performance statistics, and then use those statistics to return performance updates to the phone while safely leaving the PII on the customers' phone. Another firm, Dspark, uses a similar solution for extracting insights from highly-valued but deeply-sensitive personal mobility data. DSpark cleans, aggregates and anonymizes over one billion mobility data points every day. It then turns that data into insights on everything from demographics to shopping, which it markets to other companies — all while never selling or transferring the data itself.

Rule 3: Flows over silos. This last rule flows from the first two, and doubles as a new organizing principle for internal data teams. Once all your customer data has meaningful consent and you are acquiring insight without transferring data, CIOs and CDOs no longer need to work in silos, with one trying to keep data locked up while the other is trying to break it out. Instead, CIOs and CDOs can work together to facilitate the flow of insights, with a common objective of acquiring maximum insight from consented data for the customer's benefit.

For instance, a bank's mortgage unit can secure a customer's consent to help the customer move into their new house by sharing the new address with service providers such as moving companies, utilities, and internet providers. The bank can then act as a middleman to secure personalized offers and services for customers, while also notifying providers of address changes and move-in dates. The end result is a data ecosystem that is trustworthy, secure, and under customer control. It adds value for customers by relieving them of a burdensome checklist of moving

chores, and by delivering a customer experience that's less about mortgage rates and more about welcoming them into their new home.

The Data-Sharing Future

That last, hypothetical example is just one of the many data innovations that become possible in a new data economy based on consent, insight and flow. New companies are already springing up to provide the structures needed to facilitate these kinds of data-sharing arrangements. The emergence of data representatives, agents, and custodians make it possible to manage consent at scale, serving as trusted hubs for users' personal data and acting as their user agent in the marketplace. Data cooperatives are becoming common in some parts of the United States.

The end of the old personal data economy will not spell the end of its value creation and wealth generation; that wealth will just be distributed better and more equitably, and carry fewer privacy and security risks. People will not hoard their data assets. Instead, they'll invest them in companies that provide them with a return in the form of more and better personalized services. They may even allow those companies to share insights drawn from their data — provided the benefits accrue to them.

HR

Hossein Rahnama is Associate Professor with the Creative School at Ryerson University in Toronto and a Visiting Professor with the MIT Media Lab in Cambridge, Massachusetts. A recognized computer scientist known for his work in context-aware computing, Hossein is the founder and CEO of Flybits, a technology firm that helps companies synthesize digital customer experiences from enterprise data assets.

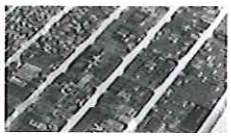
AP

Alex (Sandy) Pentland is the Toshiba Professor of Media Arts and Sciences with the Media Lab, Sloan School of Management, and College of Computing at MIT. Sandy directs MIT's Connection Science and Human Dynamics research laboratories, advises the OECD, UN, and previously AT&T, Google, and American Bar Association, and co-led the World Economic Forum Personal Data initiatives.

Recommended For You

Data Privacy Rules Are Changing. How Can Marketers Keep Up?

How to Optimize Your Company's Approach to Data Privacy



Do You Care About Privacy as Much as Your Customers Do?

Customer Data: Designing for Transparency and Trust