WHAT B2B CAN LEARN FROM B2C ABOUT DATA PRIVACY AND SHARING

By Massimo Russo and Tian Feng

This is the fourth article in a multipart series.

CONCERNS ABOUT THE SHARING of data from digital activities and devices typically focus on consumer privacy. The much discussed need for a public-health response to COVID-19 that includes widespread, automated contact tracing has brought these issues into sharp relief.

The benefits of the ability to track those who have been exposed to the novel coronavirus are impossible to deny. But so are the risks of the collected data being misused or used for purposes that the data owner neither contemplated nor intended.

The sharing of enterprise data involves similar tradeoffs between privacy and value, and balancing them requires the same level of care and forethought. The exploding volume of machine data from the Internet of Things will be used to generate high-value insights, but confidential information about companies and, potentially, employees will be at risk of misuse. With the rise of remote working, employee monitoring is blurring the boundary between personal and enterprise data.

B2B companies need a plan for dealing with IoT and other enterprise data privacy. What can they learn from the B2C experience with consumer data as they consider their own tradeoffs between protecting proprietary information and capturing value from data sharing?

The Similarities Between Personal and Enterprise Data

The focus on personal-data rights reflects the inherent power imbalance between the individuals who share their data and the corporations that use that data to deliver services. Companies are expected to be responsible data stewards, and in some jurisdictions this responsibility is enshrined in regulations such as Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act. Enterprise data is actually quite similar to personal data and likewise demands good stewardship and attention to privacy issues.

Businesses use other companies' enterprise data in many of the same ways that they use consumers' personal data: to monitor compliance, understand behavior, make predictions, and gain insights into customers or competitors. Sharing data can unlock value by improving existing offerings and creating new ones. For example, connected car data can be used to create personalized insurance policies based on driver behavior or to launch whole new mobility-as-a-service models. Similarly, machine sensors can be used not only to customize maintenance and improve quality control but also to make new options for equipment use available through pay-per-use leasing models.

But both personal data and enterprise data can be sensitive. Just as individuals might not want to reveal their income, companies typically resist revealing nonpublic, often proprietary information that could be used by competitors.

To support new uses, new data and application marketplaces and ecosystems are taking shape. A whole industry has arisen to aggregate, process, and sell consumer data in order to better understand behavior, advertising effectiveness, infrastructure utilization, and public-health policy effectiveness, among many other applications. Similarly, IoT and other enterprise data is being aggregated and analyzed for new uses. For example, the maritime Automatic Identification System, originally intended to reduce collisions by tracking the identity and location of ships, is now the source of data for a wide range of other applications, including economic analysis, insurance, and oceanic research, among others.

This is all potentially good for the economy and for business, but there are challenges to address. One is that the data is constantly being collected in the background. Both personal IoT devices and connected equipment stream data to the cloud with limited awareness on the part of their users. Once this data is aggregated, it can become harder to protect the identity of the data source and other sensitive information. And as the data is further shared, it can easily be put to uses that go way beyond what the source of the data originally consented to.

Another issue is that enterprise data can contain personal information. For example, elevator traffic information in a commercial building, coupled with business address data, could be used to track the number or identity of customers or employees visiting a company location. Street sound sensors can identify a private home where a party is taking place, and machine operations data can track operator responsiveness. Even supposedly nonpersonal enterprise data can reveal personal information when combined with inferred-identity data.

An Evolving Consumer Data Landscape

Consent is the first line of defense when it comes to data privacy. But data from connected devices can be collected without much awareness or consent. Permissions are often buried deep in lengthy legal terms and conditions. Unclear consent agreements lead to a disconnect between the data that users think is being collected and how it is being used. In many instances, users may not even be aware that they are sharing their data.

To encourage responsible data sharing, some companies have implemented best practices that consist of clear, transparent consent statements outlining what data is shared and how it is used. In Europe, the GDPR has directly addressed privacy risk by establishing the right to transparency, access, rectification, and erasure. A user may give permission to share limited data, such as whether a home is occupied, but not the identity of the resident. As data is transformed and aggregated downstream, these rights are supposed to follow the data, even as it flows through multiple intermediaries.

But personal-data ecosystems are complex and increasingly dominated by large players. The concentration of the smartphone market in many countries has led to two superplatforms—Apple and Google—that

facilitate data capture and sharing, including GPS route guidance and location data. Intermediaries have emerged that buy, aggregate, and resell data to achieve scale in both data access and analytical capabilities. Against these powerful data players, individuals have little leverage or opportunity to shape the terms of data-sharing agreements.

Consumers are discerning about how much data to share and when. Though cautious, they are largely still willing to share their data for what they view as valuable use cases. In a 2019 survey by data aggregator Acxiom (now LiveRamp Holdings), more than 80% of respondents said they were concerned about the collection and use of personal data, but 58% were willing to "make tradeoffs on a case-by-case basis as to whether the service or enhancement of service offered is worth the information requested." The business risk to companies that violate consumer trust can be high. Salesforce.com's 2019 "State of the Connected Customer" survey found that 72% of consumers would stop buying a company's products or using its services out of privacy concerns.

Lessons for Enterprise Data Sharing

B2B companies that hope to use IoT or other enterprise data in new or innovative ways should understand how evolving regulations and expectations around consumer data affect them. Rather than waiting for events to take their course, businesses can adopt best practices and self-regulatory processes to promote more robust enterprise data sharing. As companies look to balance risk and value, here are three important areas of focus.

Privacy and Intended Uses. Enterprises need to both define the rights of those that use the company's data and understand the company's rights with respect to its use of the data of others. A company that errs in either respect may incur financial and brand risk. For example, a company that makes data on factory equipment utilization available for industry aggregation purposes without proper protections could find equity traders extrapolating the company's financial performance from that data. It will be increasingly important to track the destination and uses of IoT data, especially as new use cases emerge that are very different from those that were originally envisioned. It's essential to make such information explicit not only in data-sharing agreements but also when buying equipment bundled with services that rely on the equipment's sensor data, since such equipment involves ongoing data-sharing and software-as-a-service arrangements.

Access control tools can enable permissioning in complex data-sharing setups. Just as consumers can choose to share only subsets of their personal data in order to access certain applications, enterprises may follow a similar approach with respect to IoT data, applying clear syndication rights and permissions. For example, smartphones today act as switchboards, enabling users to control which apps can access microphone, biometric, location, or camera data. Agricultural firm DKE-Data similarly enables farmers to control access to their machine and sensor data through a centralized interface, the Agrirouter. Multiple enterprise data platforms are emerging, such as Immuta and Talend, to help companies manage data rights, permissions, and syndications. As new data-sharing and aggregation platforms take shape, they will need to govern data access and use in ways that support data rights.

Value. Enterprises need to think creatively about the future value of their data. Complex ecosystems can enable data applications far from the data source, not only in the original industry but also in very different industries. Once potential use cases are identified, enterprises need to assess how critical the data is and whether substitutes are available today or will be in the future. Can the data be shared on a limited basis (such as in the form of metadata—which describes the data—or as a limited sample to invite innovation) while the company retains a financial option on the potential value of the data itself?

It will take significant effort to capture value from enterprise data. Given its heterogeneous nature, enterprise data requires more aggregation, transformation, processing, and analysis than consumer data in order to be turned into a product. In many cases, enterprises will need to invite complementary innovators to help unlock new solutions.

Sharing Options. For consumers, the core of a data-sharing decision is the tradeoff between privacy and value. A similar assessment applies to enterprise IoT data. The level of data access will vary by use case and in each instance will sit at a different point on the spectrum between capturing value and protecting privacy.

Compared with individual consumers, companies have more opportunities to monetize their data and more resources and leverage to direct the ways in which that data is shared. Realizing these opportunities will require close collaboration between legal, procurement, digital, and business teams to determine the right level of data sharing in each use case. Questions to ask include the following:

- Does the data recipient need the entire raw data set, or would a metadata description or a sample subset suffice?
- For artificial intelligence applications that require large amounts of training data, could sharing synthetic data, or data that carries the statistical properties of real data but without its privacy risk, be a viable solution?
- What about allowing algorithms to train on your data without actually sharing it, an emerging AI technique called federated learning?

Thinking deliberately not just about what data to share but about how to share it can help balance data's innovation value against the potential disclosure risk to the enterprise.

B2B companies will eventually find myriad ways to generate value by sharing data with innovation partners. But assessing the tradeoffs involved in each use case or set of permissions is at least as important for enterprises as it is for us as consumers. The experience of B2C companies —the early movers in data sharing—can help illuminate where both the potential and the pitfalls for B2B data sharers lie.

About the Authors

Massimo Russo is a managing director and senior partner in the Boston office of Boston Consulting Group. You may contact him by email at russo.massimo@bcg.com.

Tian Feng is a project leader in BCG's Boston office and a BCG Henderson Institute ambassador. You may contact her by email at feng.tian@bcg.com.

About BCG Henderson Institute

The BCG Henderson Institute is Boston Consulting Group's strategy think tank, dedicated to exploring and developing valuable new insights from business, technology, and science by embracing the powerful technology of ideas. The Institute engages leaders in provocative discussion and experimentation to expand the boundaries of business theory and practice and to translate innovative ideas from within and beyond business. For more ideas and inspiration from the Institute, please visit https://www.bcg.com/featured-insights/thought-leadership-ideas.aspx.