DATA ETHICS FOR COMPANIES

Privacy will be the number one concern over the next decade. Users and customers want to know how companies are using their data. They deserve to know exactly what is happening with their data.

How can companies respond? By ensuring an ethical, responsible data practice. Here's how.

Data has changed customer relationships

A new relationship between company and consumer has formed, and it is that of the company and user. The relationship has created:

- New expectations from users
- New responsibilities for companies to accept

The relationship already went through its honeymoon phase. There was only awe and love for the services that made it possible to buy anything on the internet, host online auctions, rent physical movies and return them when you wished, connect with friends you hadn't spoken to in years, communicate with people instantly, have access to all kinds of videos, save items on one computer and have access to them on another...and so on!

For this, there was only joy.

But now, people have adjusted. We now know these digital services a little more. The honeymoon is

over. It's no longer a love-only relationship…now, it's complicated. There is more to it. And, while companies are in a good position to carry on (financially, legally, warehouses of data, an uninformed Congress), people are withdrawing and questioning the services and practices of these companies.

To withdraw is to recognize oneself. With it are personal boundaries and the sense that one has both a private and public life. People want to:

- Reexamine the relationships they started with companies
- Hit a reset button
- Sign new user agreements

The users want data privacy. Privacy is central to leading an ethical company. But how do companies do it?

4 steps to building an ethical data practice

Data ethics and responsibility is a practice, an ongoing pursuit. Defenses like "Well the user signed the terms of service years ago" are no longer acceptable.

Today, users want to see companies respect them, respect their data, in exchange for a service that delivers value. Here are four things companies must do to respect their users:

1. Define how you use the data

Data collection is one thing, but how that data is to be used is another. Unstructured data sources allow for corporate two-facing. To avoid any misunderstanding, companies should state:

1. Exactly what data they are collecting.
2. How they will use that data.

Apple's brand new data 'nutrition label' is a start, but the label only states what is being collected—not the how. It also sets a standard for all apps on its service, but what of Apple's service itself?

2. Ask for permission

There are two aspects to getting permission from users:

1. Offer various data privacy settings to the user.
    - The basics are: "Share your data with the company", "Allow your data to be analyzed", "See your own data", "Delete all your user data."
    - Specifics will depend on the industry.
2. Ask for permission, when possible, to explore analyzing user data in new ways.

3. Respect the agreement

Trust is broken when the company breaks the user agreement. Period.

A company should not break the user agreement. If they wish to explore a new concept with services, then ask for permission.

Now, naturally, some discretion is required because of the nature of competition. The trick of the performer is to keep secrets hidden until the big reveal. And there's the fall back that goes, "It is better to ask for forgiveness, not permission".

While these might motivate a company's actions, and they believe with all their heart what they are doing will blow the user's minds, users today are exhausted and withdrawing from services at high rates. If a company chooses to break the agreement, they should recognize they give a pat on the back to a person with a sunburn. And whether those sunburned customers will return is anyone's guess.

4. Conduct good data practices

After the user accepts the user agreement, the user's data is in the company's hands. It is up to the company to handle the data responsibly. Here's how to handle data responsibly:

1. **Protect data.** While the data is in a company's possession, it's likely that the user has entrusted their data to be seen and used only by the company—not other companies the user isn't aware of. Companies should follow good data security practices.
2. **Do not share data.** User data is gathered in confidence that it is used between company and user only. Sharing or spreading that data in any other context is the equivalent to gossip and can lead to unknown consequences.
3. **Anonymize data.** Whenever data is accessed internally in any other position than direct

interactions with the user, the data should be anonymized. References to specifics can be obfuscated, abstracted, or anonymized. Personally identifiable information (PII) like names, addresses, timestamps, etc., can be blurred, not included, or randomized to keep internal company members from linking any particular data points to any user.

4. **Restrict data access.** Restrict what data is revealed to whom in the company. Certain company roles will have different levels of access. Sales teams have certain access. Customer service has certain access. Data scientists have certain access. You can define the data each role has access to by its level of detail and its level of anonymity.
5. **Conduct due diligence.** When a company passes data from one party to another, they need to do their due diligence on the company to whom they're passing the data. The user has entrusted their data with the company. They are responsible for it as long as it is in their hands. This means, if the company goes and gives it to someone who violates the user agreement, that company is on the hook—not that third party.

Restoring trust is company responsibility

I think everyone would like to see the tensions between users and companies calm down. This requires trust to be restored between both parties. If companies get disciplined about how they store, move, and provision data, create clear user agreements, and respect those user agreements, then we may see those tensions cool.

Related reading

- BMC Machine Learning & Big Data Blog
- BMC Business of IT Blog
- Data Management vs Data Governance: An Introduction
- What Is Goodhart's Law? Balancing Authenticity & Measurement
- Big Data Security Issues in the Enterprise
- What Is Data Gravity?