Towards an Ethical Application of Customer Feedback Data

Ross SMITH
Microsoft Corporation, Redmond Washington USA
rosss@microsoft.com

Abstract: Every business is a technology business. There are very few businesses that can survive without a web presence. A huge part of being a successful digital business is effective use of customer data. As more and more consumer behavior is tracked online, the reputation of a business is dependent upon it's ethical treatment of customer data. There are several categories where service operations must acknowledge and respect customer data.

***Keywords*—ethics, data, gamification, governance, customer**

INTRODUCTION

Every business is a technology business. Few businesses \can survive without a web presence, digital operations, logistics, pricing algorithms, digital payment processing, and a host of other technologies. Business is moving quickly towards the fourth industrial revolution. In 1922, in his book, My Life and Work, Henry Ford writes, "Any customer can have a car painted any color that he wants so long as it is black." Today, we have agile development processes that can respond real time to digital feedback and build new businesses real time based on customer generated data. It almost doesn't seem fair how much this new model tips the balance away from the customer. A search engine or web site can predict what the customer needs and can serve up an ad in real time to feed the desire. Business, however, is built on trust and reputation, and the online world gives new opportunities for customers to amplify their voice. A digital word of mouth campaign can take down an entire product or business – Pepsi's protest ad as an example.

We are in a new world of data, machine learning, and rapid iteration that requires an ethical approach that is constantly on display to the world.

I. Implicit and Explicit Feedback

There are several different ways to categorize customer feedback, all of which require the ethical treatment of data. Feedback data can be categorized as either implicit or explicit.

"Implicit feedback is user activity that can be used to indirectly infer user preferences, e.g. clicks, page views, purchase actions. Sometimes only positive feedback is known, e.g. the products customers have bought, but not the ones they have decided against." [1]

For the purpose of this example, explicit feedback is customer feedback given directly through available feedback channels or on social media.[2] Channels might include customer service surveys, web forms, voice or email messages.

II. Consent

Consent takes a very different form, depending on the type of feedback data that's being collected. A user filling in a web form and clicking send is, by their actions, agreeing to share the feedback with the service or firm. Many feedback forms will contain links to privacy policies or go into details on how feedback will be used. The user is giving his or her permission for the service to receive their feedback data by clicking send, or by leaving a voicemail. Here is what Bose describes about how they treat feedback data.

"Certain features of our websites make it possible for you to share comments or feedback directly with Bose or publicly with all other users of the Bose websites. Any information that you submit through such features is not confidential, and Bose may use it for any purpose (including in testimonials or other Bose marketing materials)." [3]

The story is very different for implicit feedback. The small checkbox that users click when installing an app or creating an account to use a service essentially gives permission to the service to collect usage and personal preference data. This telemetry data can be used to help improve or customize the service. So a user, by choosing one option over another is giving feedback to the service on their preference. While this data is generally anonymous, it is up to the service to follow ethical rules and behavior.

III. Privacy and Confidentiality

Almost all products and services publish their privacy policies. Because customer data is collected and valuable to the service and to others, companies take great care in abiding by privacy and confidentiality rules. Most of this policies or privacy statements will detail why and how the company may collect personal data, how they use that data, and how they may share that data.

For medical data, the "the HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically." [4]

Many data collection and storage processes will "scrub" data to remove any personally identified information. "Personally identifiable information (PII), or Sensitive Personal Information (SPI), as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context." [5]

978-1-5386-2715-0/17/$31.00 ©2017 IEEE

It's crucial that customer data be aggregated and feedback trends and tendencies viewed across data sets and not be traceable to one single user. “Pseudonymization is a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. The purpose is to render the data record less identifying and therefore lower customer or patient objections to its use. Data in this form is suitable for extensive analytics and processing.” [6]

IV. Ownership

Another area to consider is ownership of customer data. Historically, the terms and conditions require users to surrender the rights to their data to the service or company. However, legislation in Europe, known as the “right to be forgotten” law. “The right to be forgotten is a concept that has been discussed and put into practice in both the European Union (EU), and Argentina since 2006.The issue has arisen from desires of individuals to "determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past.” [7]

This has opened a new look into ownership practices, where some services allow customers to request to have their data removed from storage. Ethical behavior on the part of the services allows customers full control and ownership of the data they generate. More recently, The General Data Protection Regulation (GDPR) aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. [8]

The rules around ownership of personal data are changing, with more power and control given back to the user.

V. Accountability

Ethical service operators will treat customer data with respect and hold themselves accountable for it’s use, how and where data insights are applied, and remain accountable to keep user data secure.

Walmart, for example, has a Pledge of Accountability: “We require our associates, business partners, and service providers to manage your personal information properly.

We have designated a team of trained associates who are responsible for helping to ensure compliance with this Policy. We require all those who manage customers’ personal information to do so properly and in accordance with our policies.” [9]

An example of not being accountable would be a search provider selling the identities of users who search for “cancer symptoms” to insurance companies

VI. Data Governance

“Data governance is a defined process an organization follows to ensure high quality data exists throughout the complete lifecycle. The key focus areas of data governance include availability, usability, integrity, and security.” [10]

Ethical use of data requires that service providers and companies have clear policies for who has access to customer data, what levebls of personal information are available to certain classes of employees, security clearances, and transparency policies. It’s important to plan ahead for scenarios where employees have access to personal data. When possible, all personally identifiable information (PII) should be removed before employees are given access to the data. In addition, regular reviews of data governance policy should be held and extend to any partners or collaborators who have access data. In addition, if any customer data is to be sold, partner requirements should be outlined and evaluated.

Many data governance programs are driven by the need to comply with government regulations. Examples include GDPR, Sarbanes-Oxley, HIPAA, and others around the world.

VII. Security

While it would seem obvious that the ethical treatment of customer data would include keeping it secure, there are regular stories in the press about security breaches or hackers getting away with millions of credit card records.

Customers trust the reputation of the services they share btheir data with. Service providers and businesses build their reputation on the service they provide to customers, and if they are unable to keep their data secure and safe from hackers or misuse, they risk the core of their business.

VIII. Sharing and Transparency Policies

Service providers often re-sell customer data to other companies. This can range from legitimate to often questionable marketing practices, where a company may require a valid email address for account security, and then sell that email address list to markets preparing online email campaigns. It’s important for the ethical use of customer data for services to be transparent in how and what information they will share with others.

Netflix policy describes how it disclosures information [11] We disclose your information for certain purposes and to third parties, as described below:

- The Netflix family of companies
- Service Providers
- Promotional offers
- Protection of Netflix and others
- Business transfers

Most services and product companies are clear in their privacy statements about how, where, and why they are sharing customer data. An ethical approach towards customer data includes being transparent about the circumstances under which data will be shared.

There are a number of court cases surrounding tech companies legal requirement for sharing with law enforcement. Ethical behavior is sometimes subject to extenuating circumstances and can quickly become a slippery slope.

IX. Reporting

Reporting on customer trends is generally done in aggregate. There are not many business insights to be gained in a report that says that Bob and Mary Smith made 4 visits last week. In 2012, Rocky Mountain Power in Utah, started a pilot showing a household's power consumption relative to the neighborhood average. An aggregated or pseudonymization of individual data to provide better insight.

It's important that individual data not be shared. Online services give us new insight into human behavior, but to be ethical is to maintain respect for the individual and to use the data to help the experience while retaining privacy.

X. Conclusion

Looking back to Socrates, Plato, and Aristotle, and their work on ethics, virtue, and living well, we can build a strong foundation of principles for how to treat customer data. It's very easy to say "just do the right thing", but circumstances like the San Bernardino shootings [12] show that there is often not a clear case for what the right thing is. There have been a few instances of data science groups developing their own "Hippocratic Oath" [13] and frameworks like this may help when the technology – and the bar for what's acceptable – is moving so fast. Common sense, empathy, and the "Golden Rule" will cover 90% of the cases, and that's a good start.

As more business moves online, and more human processes become virtualized and automated, it's critical that an ethical approach to data collection, analysis, reporting, sharing, and dissemination be built into every business plan.

References

[1] http://recsyswiki.com/wiki/Implicit_feebdback
[2]https://www.joshsteimle.com/entrepreneur/two-types-of-customer-feedback.html b
[3] https://www.bose.com/en_us/support/your_privacy_rights.html
[4]https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es
[5] https://en.wikipedia.org/wiki/Personally_identifiable_information
[6] https://en.wikipedia.org/wiki/Pseudonymization
[7] https://en.wikipedia.org/wiki/Right_to_be_forgotten
[8] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
[9] https://corporate.walmart.com/privacybb-security/walmart-privacy-policy
[10] https://en.wikipedia.org/wiki/Data_governance
[11] https://help.netflix.com/legal/privacy
[12] https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone
[13] https://www.techatbloomberg.com/blog/data-scientists-develop-version-hippocratic-oath/