Data Governance – A case study: Legal obligations and ethical challenges

Merrimack College

Data Governance, Laws and Ethics

Amol Gote

April 26th, 2020

Recent advances in big data has resulted in new laws been passed and have posed organizations with new ethical challenges, so in this context this paper focuses on the Fintech startup referred to as "XYZ" henceforward. XYZ provides the capability to originate and finance personal loans at the point of care, in this case at a dentist's office through a mobile or an iPad application. XYZ has a tie-up with various dentist networks with which numerous dentists are affiliated with. The purpose of these loans is for a variety of dental treatments like braces, crowns, bridges, etc. Once a loan is approved, it is underwritten by a primary bank and then this loan is bought from the primary bank by other partner banks with which the XYZ has a contractual agreement. The XYZ organization acts as a mediator between various loan buying banks and dentist networks. In this personal loan life cycle, XYZ collects its customers (in this case dentist patients) data in 2 stages. The first stage is a loan application where it collects personal data such as first name, last name, SSN, date of birth, address, and income. It pulls and stores their credit reports, gathers additional information like education, employment, its dentist association, scanned Identity documents like driver's license. The second stage is loan repayment where XYZ captures bank account details, monthly transactional records, payment history, etc. In short, there is a lot of data in play, whether it is PII data or financial transaction data.

XYZ collects personal and financial data so it falls under the purview of FTC and must abide by the Gramm-Leach-Bliley Act (GLB Act). "*The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.*" *(ftc.gov).* GLB Act requires certain safeguards in place, that prevent unauthorized access to customer's PII data. As XYZ is involved in credit decisioning, it must fulfill FCRA requirements. *"The Fair Credit Reporting Act (FCRA) is a federal law that regulates the collection of consumers' credit information and access to their credit reports." (Kagan, 2019).* XYZ has access to customer's credit reports which contains information about credit cards (AKA trade lines), mortgages, loans, account opening dates, credit limit, credit scores, account balance, number of credit inquiries, bankruptcies, etc. All this information needs to be protected and managed securely. XYZ has a contractual obligation from the credit bureaus on the usage of various data elements from the credit report for business analytics. E.g. FICO which is a credit score to determine the creditworthiness, can be used for credit decisions to offer the best possible loan option to the customer, but it cannot be used internally by XYZ to perform any kind of analytics or reporting. XYZ needs to abide by state-specific laws, e.g. it validates the identity of the customer electronically by comparing the driver license image uploaded by the applicant and selfie taken during the application process, and in this procedure XYZ stores selfie image as well as driver license image. Illinois Biometric Information Privacy Act (BIPA) states that *"Biometric Data will be destroyed when no longer needed for the initial purpose for which it was collected, and in any event within three years of the subject's last interaction with the company." (McInerney, 2019)*. So, XYZ must delete the selfie and driver license image after 3 years, so that they are compliant to BIPA. Whereas other states do not have such requirements, so data retention policy differs across states.

XYZ has been reasonable, at complying with these various laws, being a cloud company, they are leveraging best practices from the cloud provider to protect unauthorized access to any kind of data. They have data classification in place, all the PII and high-risk data fields are encrypted in the database. Identity documents, biometric data, and credit reports are stored using a secure storage service and are encrypted at rest. Data transfer to various partner banks is through API's and these have 2 levels of security infrastructure, firstly IP based filtering, and secondly token (OAuth) based authentication. The Mobile application leverages secure API's where transport-level security is guaranteed by SSL. Despite all these safeguards, there are possibilities of security lapses due to their day to day operational activities or new deployments for their product and these can be avoided by incorporating a data governance framework.

Along with data security, there are ethical challenges as well for this organization. To elaborate let us shed light on some examples. The First one is XYZ encourages its customers to set up autopay and give a 0.5% interest rate discount if autopay has been set up. For performing autopay set up, XYZ product uses third party services like Plaid or Fincity, which provides the ability to connect to bank accounts by entering the online login credentials. After the account is linked by entering bank-specific credentials, XYZ validates the account ownership and gets the account information for monthly autopay set up. It also enables, XYZ to access customer's bank related transaction records and it can easily pull the latest transactions. The customer has not signed up for this, even though it might have been mentioned in the autopay consent somewhere. This transactional data collected by XYZ could be used for credit decisions for subsequent loans which could affect the rate of interest positively or negatively. XYZ can also sell this information to Partner banks which are big or mid-sized financial institutions, that could then use this data to target their banking related products through XYZ mobile app. Throughput this process, the end-user is unaware that the data that he or she owns is extracted and utilized by a third party. The Second moral challenge for XYZ is location data it gathers from the mobile application. To find the dentist's location, the mobile app needs access to location service, once the access is granted mobile app can gather the location information whenever the app is accessed. This location data can then be sold to the data aggregation companies who then can offer the data to advertising companies that are looking for consumer information and trends associated with them. XYZ can use location data to promote its products e.g. if a customer visits a dentist's office there could be an in-app notification to check with the user to see if they need a loan. Third ethical data challenge for XYZ is how to limit the use of credit bureau report data, it contains valuable information about the credit history of the customer, by contractual agreement with credit bureaus they cannot use certain information from credit reports for analytics and reporting, but nothing is stopping them from using alternate information from bureau report like payment history, mortgage accounts, credit card accounts. They can sell this information to partner banks for targeting their products through the mobile app. The Mobile app provides XYZ access to various other personal information of customer which is sitting in the device, the app has a feature to add co-applicant which can be done by sending a message to co-applicant through your phone contact list, this way application gets access to all the contacts of the customer. The App needs access to all SMS data if the customer wants the app to auto-fill the one-time password for bank-related transactions, now the app has access to all the SMS messages as well. So far XYZ has not used all this information gathered through the device for any commercial purpose, but that does not guarantee that they might not do in the future. Another challenge for XYZ is to avoid any biases in credit decisions based on personal characteristics. XYZ is currently using standard rules-based credit decision policy for approving the loans, but eventually, with data they accumulate, they want to move towards AI/Machine learning based algorithm to make the credit decisions, now these algorithms need to ensure that they are not discriminatory based on certain attributes of the customers e.g. gender.

In conclusion, XYZ has been going by the book and following all financial and credit-related laws and safeguarding the PII information of the customer. It is a startup, but as it matures and with sound data governance framework in place, it will mitigate the risks of data breaches. It sits on a pile of customer data gathered through a mobile app, credit bureau, and customers, some of which it is legally obligated not to be used commercially, but for remaining it’s up to XYZ how ethically they should use the data. XYZ claims to be a customer-centric organization so by this philosophy they must respect the privacy rights of their customers.

Bibliography

FTC.gov. *Gramm-Leach-Bliley Act.* Retrieved from FTC website: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

Kagan, J. (2019, May 14). *Fair Credit Reporting Act (FCRA).* Retrieved from Investopedia: https://www.investopedia.com/terms/f/fair-credit-reporting-act-fcra.asp

Groot, J. (2019, July 15). *What is GLBA Compliance? Understanding the Data Protection Requirements of the Gramm-Leach-Bliley Act in 2019.* Retrieved from the digital guardian: https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act

McInerney, S., Malhotra, G., Craig, D. (2019 Jan 31). *In Landmark Case, Illinois Supreme Court Sets Low bar for Claims Under Illinois' Biometric Information Privacy Act Biometric Information Privacy Act.* Retrieved from textcase: https://casetext.com/analysis/in-landmark-case-illinois-supreme-court-sets-low-bar-for-claims-under-illinois-biometric-information-privacy-act-1

CBS News. (2019, April 29). Whistleblower reveals info on companies buying and selling your location Data. Retrieved from CBS News: https://www.cbsnews.com/news/location-tracking-whistleblower-reveals-info-on-companies-buying-and-selling-your-location-data/

Privacy Rights org. (2018 Dec 28). *Credit Reporting Basics: How Private Is My Credit Report?* Retrieved from privacyrights.org: https://privacyrights.org/consumer-guides/credit-reporting-basics-how-private-my-credit-report

U.K. Finance, KPMG. (2019 March). *Ethical use of customer data in a digital economy*. Retrieved from KPMG: https://assets.kpmg/content/dam/kpmg/uk/pdf/2019/04/ethical-use-of-customer-data.pdf