

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

Merrimack College

Data Governance, Laws and Ethics

Amol Gote

April 5th, 2020

This paper focuses on the Fintech startup referred to as "XYZ" henceforward, it 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 various dentist doctors are affiliated with. Purpose of these loans is for various kinds 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 XYZ has a contractual agreement. XYZ organization acts as a mediator between various loan buying banks and dentist networks. So, in this entire 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 first name, last name, SSN, date of birth, address and income, it pulls and stores their credit reports, gather additional information like education, employment, its dentist association, scanned Identity documents like driver’s license. The second stage is loan repayment where it captures bank account details, its monthly transactional history, payment history, etc. For loan repayments as it needs to co-ordinate transactions with loan buying partner banks and primary data bank. So, in short, there is a lot of data in play, whether it is personal 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.*” *(www.ftc.gov).* GLB Act requires certain safeguards in place which avoids unauthorized access to customers PII data. Apart from the personal and financial data, they are involved in credit decisions, so they 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.” (Investopedia, 2019).* Apart from PII information credit reports 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. Apart from FCRA compliance, XYZ has contractual obligations from bureaus on the various data elements from the bureau report will be used for reporting or 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. There are state-specific laws to which XYZ needs to respect, e.g. XYZ validates the Identity of its customer electronically through driver license upload and comparing with the selfie taken during the application process, it is storing 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.”* *(Casetext 2019)*. So, it needs to delete the selfie image and an extracted photo from driver’s license after 3 years and other states do not have similar requirements, in this case, data retention policy varies across various states.

XYZ has been pretty good at complying with these various laws, they are cloud company, so they are leveraging all kinds of 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, Credit reports are stored using 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 is in place, 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 of all these safeguards in place, there are still 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 data governance framework.

Apart from data security, there are ethical challenges as well with this organization. Let’s look at a couple of 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. This also provides XYZ access to customers banks related transaction history and it can poll regularly to grab 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 interest in a positively or negatively. Apart from this XYZ could 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. In this whole cycle, the end-user is unaware that the data that he or she owns is extracted and utilized. The Second moral challenge for XYZ is location data it gathers from the mobile application, for finding dentist location mobile app needs access to location service, once the access is granted mobile app can gather always 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. Apart from this 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 any need for a loan. Other ethical data challenge with 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, so in doing so application gets access to all the contacts list 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. So far XYZ has not used this information gathered through the device for any commercial purpose, but that does not guarantee that they might not do in the future. Another test for XYZ is to avoid any biases in credit decision based on personal characteristics, XYZ is using currently standard rules based credit decision policy for approving the loans, but eventually with data they accumulate, they want to move towards AI/Machine leaning 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.

Finally, to summarize XYZ has been going by the book and following all financial and credit-related laws and safeguarding PII information of the customer. It’s a startup, but as it matures and with sound data governance framework in place, it will mitigate the risks for 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 much ethical they need to be with that data. It must practice fairness and respect the privacy rights of their customers.

# Bibliography

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

[advice/business-center/privacy-and-security/gramm-leach-bliley-act](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-](https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act)

[requirements-gramm-leach-bliley-act](https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act)

Malhotra. G., Craig. D., McInerney. S. (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-](https://casetext.com/analysis/in-landmark-case-illinois-supreme-court-sets-low-bar-for-claims-under-illinois-biometric-information-privacy-act-1)

[court-sets-low-bar-for-claims-under-illinois-biometric-information-privacy-act-1](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-](https://www.cbsnews.com/news/location-tracking-whistleblower-reveals-info-on-companies-buying-and-selling-your-location-data/)

[whistleblower-reveals-info-on-companies-buying-and-selling-your-location-data/](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-](https://privacyrights.org/consumer-guides/credit-reporting-basics-how-private-my-credit-report)

[private-my-credit-report](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-](https://assets.kpmg/content/dam/kpmg/uk/pdf/2019/04/ethical-use-of-customer-data.pdf)

[data.pdf](https://assets.kpmg/content/dam/kpmg/uk/pdf/2019/04/ethical-use-of-customer-data.pdf)