Date: July 24th, 2023
To: Bob Partner, Capital LLP
From: Jacqueline Ocaña, Ethics and Policy Intern
RE: CodeTech's Identified Ethical, Security, Privacy, and Risk Issues Need Improvements

---

**CodeTech Launching Friendship Augmenting Product, Clairvoyant, Seeking Funding**

CodeTech is a software development company, founded by Betty and Pierre, based out of San Francisco looking for funding to launch their first product, Clairvoyant. Clairvoyant aims to disrupt the dating application market with its focus on connecting people to build friendships over romantic relationships. CodeTech's target markets are located in the United States and Europe and identified to be in the LGBTQ+ community.

Clairvoyant created an algorithm that is used to identify individual traits such as when someone is generally happy, sad or self-confident, to their political perspective, or even their sexual orientation. Since it is currently focused on the LGBTQ+ community, sexual orientation is being predicted by the algorithm based on the data provided to it from external professional sites such as LinkedIn and NextDoor.

**Clairvoyant Collects Several Types of Sensitive Personal Information**

Through the Clairvoyant product, CodeTech collects the following data about their users:

- Images of user's face
- Zip code
- Predicted political perspective
- Predicted sexual orientation
- Predicted individual traits (happy, sad, self-confident, and others not specified)
- Name
- Gender
- Age
- Address
- Email address
- All subscriber search queries within product
- Username and passwords for any protected sites they wish to connect (Nextdoor, LinkedIn)
- Information scraped from professional platforms
- Credit card information

Data is stored on servers in the United States. None of this data is encrypted. This data is considered sensitive personal information which is protected by specific legislation.

**CodeTech Must Adhere to the CCPA, GDPR and PCI Regulations**

Based on the information mentioned above, such as geographic region and sensitive personal information data, CodeTech's product, Clairvoyant must, at minimum, adhere to the following forms of governance:

- California Consumer Privacy Act (CCPA) - While specific to only California users, this act is more comprehensive than the federal regulations and can cover the entirety of the United States. This is due to CodeTech entering the United States market, including the state of California.
- General Data Protection Regulation (GDPR) - This protects the users located within Europe. This is due to CodeTech entering the European market.
- Payment Card Industry Compliance (PCI) -This protects the credit card information that will be used to pay for user subscriptions. This is due to CodeTech entering the United States market.

**CodeTech Currently Violates CCPA, GDPR and PCI Regulations**

The practices currently in place by CodeTech and Clairvoyant violate the following:

- Uses ARCP, third party vendor, for data storage, without data encryption on any information. This violates the regulations in both PCI and CCPA as they handle financial data which is protected under this regulation.
- Users are not specified what personal information is being collected: violates the right to know in the CCPA and GDPR.
- Failure to include text regarding how to change preferences surrounding how personal information is used: violates right to delete, op-out, correct information, limit use of sensitive personal information, access information related to automate decision making, opt out of automated decision making, and data collection minimization within the CCPA and GDPR.

**CodeTech's Privacy Policy is Lackluster, Insufficient, and Deceptive**

CodeTech admits that it has not prioritized privacy for Clairvoyant, however some measures were taken to address it. CodeTech consulted with a third party company, Utah Data, to develop a privacy policy for Clairvoyant.

Utah Data is a company that provides services solely in Utah. CodeTech borrowed Utah Data's current privacy policy and placed it on Clairvoyant's site without review. The privacy policy is insufficient to cover Clairvoyant. Utah Data does not need to abide by the CCPA and GDPR as they are solely based and operate in Utah. Clairvoyant would need to abide by the CCPA and GDPR because they operate in multiple different locations throughout the world.

**Major Limitations Found in CodeTech's Privacy Policy**
Looking deeper into the policy the following limitations are found:

- "We collect Subscriber personal information only to provide our services, improve Subscriber experience, and or fulfill our legal obligations."
    - *CodeTech fails to mention they intend to sell information to data brokers. This is a transparency issue for the company.*
- "We do not share personal information with third parties that are not associated with providing our services to our Subscribers. Subscribers can be assured that we will never sell your personal information."
    - *CodeTech admits they will be selling information collected to data brokers. CodeTech fails to mention data is also being shared with third parties like their third-party cloud provider, ARCP, in addition to data brokers. This is a deceptive and unfair practice that violates this policy.*
- "Subscriber information is only retained for as long as it is necessary to provide services to you, improve user experience or fulfill legal obligations, after which we take reasonable steps to destroy the data so that it cannot be accessed or misused by any unauthorized party."
    - *CodeTech admits they will not be destroying any of the data they obtain. This is a deceptive tactic.*
- "We take all reasonable steps to ensure that any personal information we collect, or share is accurate and suitable for the services that we provide to you."
    - *CodeTech currently does not encrypt any of their data lacking protection of data. This is contrary to what is stated and is deceptive for the user.*

**CodeTech Lacks Any Written Policies Surrounding Risk Assessments, Procedures and Controls**
ARCP, the third party cloud provider for CodeTech, has implemented "independent audits and certifications to demonstrate compliance with industry-recognized security standards and regulations," however this only applies to the portion that ARCP is involved with. As a result, ARCP recommended Clairvoyant be assessed by an independent security third-party. Clairvoyant declined the recommendation as they had already used SSF, a small security firm, "to see what level of effort and cost it would take to get an independent security certification based on common security standards and regulations." CodeTech was advised by SSF to implement "risk assessment, written security policies and procedures and all sorts of controls like intrusion detection and monitoring systems" which CodeTech refused to implement in any capacity. This puts user data at severe risk as it is not being managed and protected properly.

**Recommendations Before Funding is Granted: CodeTech Must Adhere to Regulations, Establish WrittenPolicies and Procedures, and Edit Current Privacy Policy**

Based off the information established, I would recommend that CodeTech implement the following steps before Capital, LLP considers investing in CodeTech's product, Clairvoyant:

- Adhere to the most recent California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), and Payment Card Industry Compliance (PCI) laws with all of the sensitive personal information collected from users.
- Revise their current privacy policy to include information on third party vendors and business partners, data selling practices, storage and deletion of data, data encryption and remove any deceptive language.
- Establish risk assessment, written security policies and procedures, and controls taking place. Ensure this is done systemically and periodically.