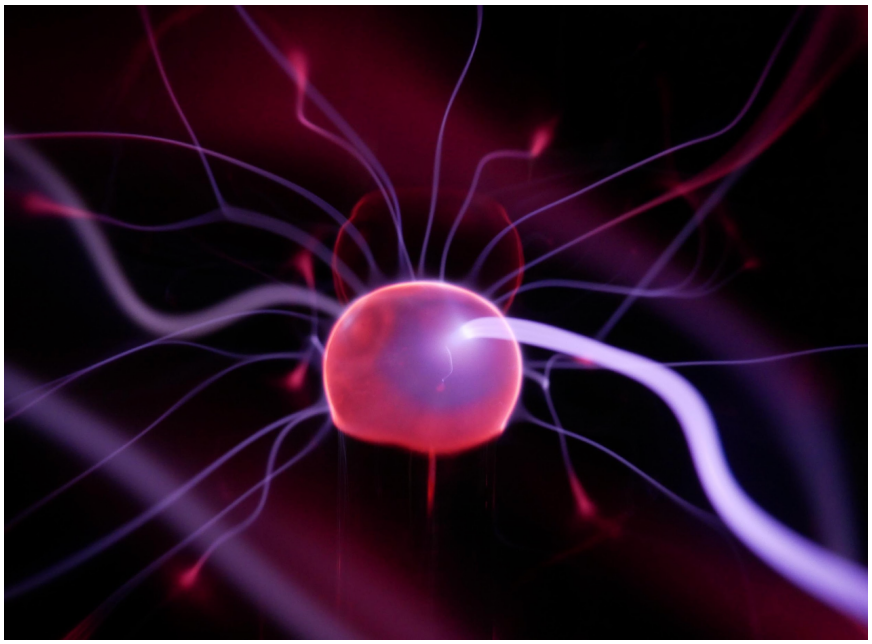

Surge Consulting

Expansion Proposal

Prepared for Tachyon Tech

Created by Ali Jamil & Jaquasia Donald

01/22/2023

Regulatory Bodies

Tachyon Tech is a small company that operates in the state of California and Germany which means they are liable to the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). These two respective data privacy laws enforce rules independently of each other but this company is responsible for complying with both, as a multinational organization. Although there is no current country-wide federally placed data privacy policy, there are industry-based privacy regulations like HIPAA and FERPA. Leaving the decision up to the states, and on a global scale it leaves room for regions to decide upon their own mutual agreement. If Tachyon Tech were to conduct business with any other country or region in any capacity then they must also comply with the laws there. This could involve offering goods or services to that region and collecting data from individuals residing there.

The GDPR is an E-wide privacy law that imposes data security and privacy measures within companies to protect individual rights to their own data. This law was created by the European Parliament and the Council of the European Union. Currently, the regulations are being enforced by the Information Commissioner's Office (ICO). This is the entity that is responsible for investigating any misconduct and can issue out large fines if the company is found to be in violation. Companies that are expected to comply are those that collect, process and store the data of EU citizens. This includes abiding by clear consent requirements, privacy by design, and a mandatory timely data breach notification (Heine, 2021). It is required that each EU member state designate the role of monitoring GDPR compliance to an individual Data Protection Authority (DPA) (https://kirkpatrickprice.com/blog/whos-enforcing-gdpr/). These national supervisory authorities monitor how regulations are being applied and if it respects

individual data rights under the law. This law also calls for companies to appoint a Data Protection Officer (DPO). The role of a DPO involves training staff in proper data processing, conducting audits to ensure compliance, and monitoring the performance of data protection efforts (Lord. 2021). Among these responsibilities, a DPO also must serve as the point of contact between the company and the appointed DPA. If a DPA would like to further investigate the company's activities, the DPO is responsible for providing a comprehensive list of records conducted by the company. The implementation of GDPR rules applies to all personal data collected. Personal Data can include names, location information such as IP addresses, and even images. Genetic, biometric, and health data are protected as personal data as well.

The CCPA is a state-enforced data privacy law that grants more rights to individuals in California regarding their data and Personal Information (PI). Consumers have the right of notice meaning businesses must clearly inform users before collecting data and through the right of access they must disclose what categories of personal data will be stored. This law ensures the right to opt in or out at any time and the right to request the deletion of personal information if consent is revoked. California residents have the right to be notified in the case of a data breach as it relates to the security of their PI. All consumers have the right to equal services and prices if they decide to exercise their right to decline participation in the use or sale of their data (Bruemmer, 2019). The CCPA defines Personal Information as any information that could identify, link to, or possibly be associated with a particular consumer (Torre, 2019). This includes direct or unique identities, biometric data, geolocation, internet activity, or sensitive information. Within these categories, some examples are names, IP addresses, voice recordings, location history, browsing history, and health data respectively. The CCPA was amended in 2020 by the

California Privacy Rights Act (CPRA). The CPRA created the California Privacy Protect Agency which was granted “full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018” (California, 2023). Although by the CCPA, the California Attorney General still retains enforcement powers. The CCPA and CPRA impose certain obligations on businesses, service providers, third parties, and even contractors. If one of these entities listed is found to be in violation there are many different consequences. There are civil penalties with the option to solve alleged violations within 30 days of notice, statutory damages no greater than $750, and non-monetary relief in the case of security breach violations. Among the options listed, entities being held to the CCPA and CPRA may also be subjected to an injunction in actions brought by the Attorney General (Wilmer, 2023)

Impact of Data Regulation

A survey done by ESET reveals many businesses operating in California are still in the dark about CCPA even though it affects them directly. After receiving responses from 625 business owners and executives, they found 44% of participants have never heard of the CCPA. Also, it was found, of the total, 34% of participants said they didn't know if there needs to be changes made to their business protocols to how they capture, store, and process data to comply (Burkette, 2019). Meaning many businesses are unaware of the magnitude of changes the CCPA ensues over their company in regards to data privacy protocols. As Tachyon Tech continues to operate in any capacity in California or with its residents, this company must conduct business in ways that do not break this law.

Due to the CCPA constraints companies are exposed to being sued by consumers if they lose a customer's data/information. This will encourage companies to improve their security measures, which in turn benefits the consumer. As litigation increases, more consumer rights are being created and protected, and small companies must start thinking about personal data being processed and protected within their company. Beyond the case of lack of awareness, many small businesses cannot afford to expend resources on diving into big data. If they do, they must also afford the time, staff, and money to maintain CCPA/CPRA compliance. Fortunately, consumers respond positively to companies that are transparent about privacy policies, cookies, and other forms of data collection (Label Insight, 2018). If regulations were to become more restrictive in many ways, companies may have to adapt how they ask for consent to collect data from users. This could make it more complicated and consequently receive fewer opt-ins for their policy agreements.

If Tachyon Tech were to use tracking cookies to record user data for marketing purposes in Germany they would need to comply with the GDPR. Beginning to implement GDPR regulations will allow a company based in the United States to be prepared for expanding internationally. When the GDPR took effect for the EU and the UK it also subjected companies all around the world to its rules as well. If restrictions were to become far more rigid than Tachyon Tech would begin by conducting a data audit to examine the current measure that could be considered a violation. The large encompassing GDPR upgraded how companies treated data security, and any further changes would require some effort to adapt to. If restrictions were to loosen perhaps companies would still choose to conduct business to the current standards they are used to instead of downgrading. Although more likely, looser restrictions would cause

individuals to lose certain rights they have now depending on the change. Stricter and more complex data privacy laws leave small companies behind because of the confusion and lack of knowledge, as well as the enormous effort it takes to begin collecting, processing, or storing consumer data lawfully. It is important for Tachyon Tech to comply with the CCPA/CPRA and GDPR laws as an international commercial company operating in California and Germany.

Regulating Data Usage

The GDPR pertains to two types of data, personal data, and sensitive data. The GDPR goes on to define sensitive data as consisting of racial/ethnic origin, religious beliefs, genetic/biometric data, or data involving health. Non-sensitive data is not directly identifiable information but still allows for the analysis of individual behavior. This can include cookie IDs, censored email addresses, or any identifiers that don't directly reveal the true individual associated with it (“GDPR sensitive and non-sensitive data,” 2018). Tachyon Tech may decide to collect sensitive data to further market their consumers advertisements or new products based on their address, ethnicity, or even health information. Collecting sensitive data could provide Tachyon Tech with the information to improve its customer experience by modifying its presence, goods, or service.

When collecting sensitive data companies should also practice encryption which converts data into unreadable code that requires a password to read. Although it requires more work to prepare the data appropriately, sharing personally identifying information (PII) is possible. One way to share sensitive data involves de-identification. This process removes direct identifiers

which are usually not needed in the analysis process and uses non-identifying numbers to differentiate between records. Or it could involve aggregating values by using scales and ranges such as age range. Continuing to transform the data to reduce precision can act as an additional de-identifier, for example; generalizing responses, removing outliers, and grouping geo-bordered regions ("Guides: Creating inclusive surveys," 2022). The challenge of collecting sensitive data is taking on the risk of harm to consumers if their data were to be breached, even on the smallest scale. Meaning companies take on more liability if they decide to collect sensitive data from their users

The process of collecting non-sensitive data does not take as much effort since the restrictions are looser. Non-sensitive personally identifiable information (PII) can be easily accessed from public sources (like phonebooks), which proves the difference in leniency. It is because it can not be used alone to identify a consumer (Frankenfield, 2022). Companies that choose to collect this type of data because it is less risky will also face the consequence of shallow analysis. Non-sensitive data has limits and may not be as useful to researchers to investigate complex patterns of behavior. The potential of this data is limited because of the vagueness that allows it to be unidentifiable alone.

Data Professional Roles

A company should create a designated team of individuals who are responsible for data security management. At the top of this team, there should be a Chief Information Security Officer (CISO) to lead and direct all efforts. This role must manage to create the appropriate

policies and any strategies necessary to secure data from possible threats. The CISO is also responsible for communicating relevant updates to executives and any recommendations to improve the workflow. On the IT team, there should be a director that enacts the strategies devised, monitors activity within the IT infrastructure, and implements security technology that covers the whole organization (Spirion, 2021).

The GDPR requires all companies to designate a Data Protection Officer (DPO) who is in charge of overseeing data protection strategies and their implementations. The DPO also acts as an intermediary for the company and Data Protection Authorities (DPA) appointed by each EU member state. To stay in compliance with the GDPR companies can hire a controller (person or entity) that decides the methods to properly process personal data. A Supervisory Authority is a public authority that advises companies, addresses complaints, and issues fines. This role is also referred to as a DPA (Ground Labs, 2021).

There are platforms and data management systems available for companies to take advantage of to expedite and simplify the process of discovering sensitive data. Choosing to implement a system to manage privacy compliance and data protection processes allows companies to satisfy CCPA/CPRA and GDPR requirements. Softwares monitor controls to secure data, track consumers who opt-in or opt-out of the sale of PII, and manage consumer data flows within all systems. Beyond automation tools, companies can seek outside help by contracting a specialized officer to fill the position of a DPO. An external DPO will give advice, coordinate data loss prevention strategies, and assist in training staff. A company may explore

external help to process the large amounts of sensitive data that are being stored (DataGuard, 2022).

References

Bruemmer, E. (2019). *Consumer rights under the CCPA, part 1: What are they?: Davis Wright Tremaine*. Privacy & Security Law Blog | Davis Wright Tremaine. Retrieved January 22, 2023, from https://www.dwt.com/blogs/privacy--security-law-blog/2019/07/consumer-rights-under-to-ccpa-part-1-what-are-they

Burkette, R. (2019, August 5). *ESET survey reveals widespread business confusion about upcoming CCPA regulation*. Business Wire. Retrieved January 22, 2023, from https://www.businesswire.com/news/home/20190805005132/en

California, S. of. (2023). *Regulations*. Regulations - California Privacy Protection Agency (CPPA). Retrieved January 22, 2023, from https://cppa.ca.gov/regulations/

DataGuard. (2022, November 11). *External Data Protection officers: An overview*. DataGuard. Retrieved January 22, 2023, from https://www.dataguard.co.uk/blog/external-data-protection-officers-an-overview

Frankenfield, J. (2022, November 22). *What is personally identifiable information (PII)? types and examples*. Investopedia. Retrieved January 22, 2023, from https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp

GDPR sensitive and non-sensitive data: A distinction with a difference. Criteo. (2018, April 14). Retrieved January 22, 2023, from https://www.criteo.com/blog/gdpr-sensitive-non-sensitive-data-distinction-difference/

Ground Labs. (2021, May 3). *Who is responsible for GDPR compliance at your company?* Ground Labs. Retrieved January 22, 2023, from https://www.groundlabs.com/blog/gdpr-responsibility/

Guides: Creating inclusive surveys: Collecting sensitive data. Collecting Sensitive Data - Creating Inclusive Surveys - Guides at Penn Libraries. (2022). Retrieved January 22, 2023, from https://guides.library.upenn.edu/inclusive-surveys/sensitive-data

Heine, I. (2021). *3 years later: An analysis of GDPR enforcement: Strategic technologies blog*. CSIS. Retrieved January 22, 2023, from https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement

Label Insight. (2018, June 29). *Study: Nearly three-fourths of consumers would pay more for products that offer complete transparency*. STUDY: Nearly Three-Fourths of Consumers Would Pay More for Products that Offer Complete Transparency. Retrieved January 22,

2023, from https://www.prnewswire.com/news-releases/study-nearly-three-fourths-of-consumers-would-pay-more-for-products-that-offer-complete-transparency-300318901.html

Lord, N., Zhang, E., Groot, J. D., & Lord, N. (2022). *What is a Data Protection Officer (DPO)? learn about the new role required for GDPR compliance in 2019*. Digital Guardian. Retrieved January 22, 2023, from https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance

Spirion. (2021, September 7). *Who is responsible for Data Security & Compliance*. Spirion. Retrieved January 22, 2023, from https://www.spirion.com/blog/who-responsible-data-security-management-compliance/#:~:text=A%20company%27s%20CISO%20is%20the,plan%20if%20the%20worst%20happens.

Torre, L. (2019, September 30). *What is "Personal information" under CCPA?* What is "personal information" under CCPA? – California Lawyers Association. Retrieved January 22, 2023, from https://calawyers.org/antitrust-unfair-competition-law/what-is-personal-information-under-the-california-consumer-privacy-act/

Willmer, Z. T. and S., Chen, V., & Headley, T. (2023, January 20). *What's the difference between CCPA & CPRA*. Bloomberg Law. Retrieved January 22, 2023, from https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/#:~:text=Although%20the%20CPRA%20grants%20the,Code%20%C2%A7%201798.199.