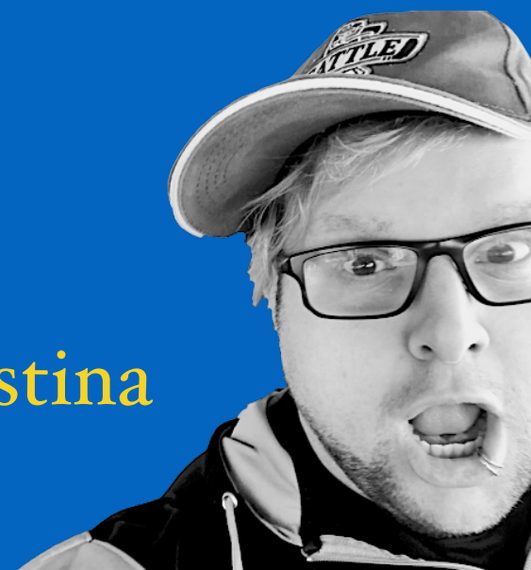
# Concerning a User Database

Joseph T. Cristina



# User Database

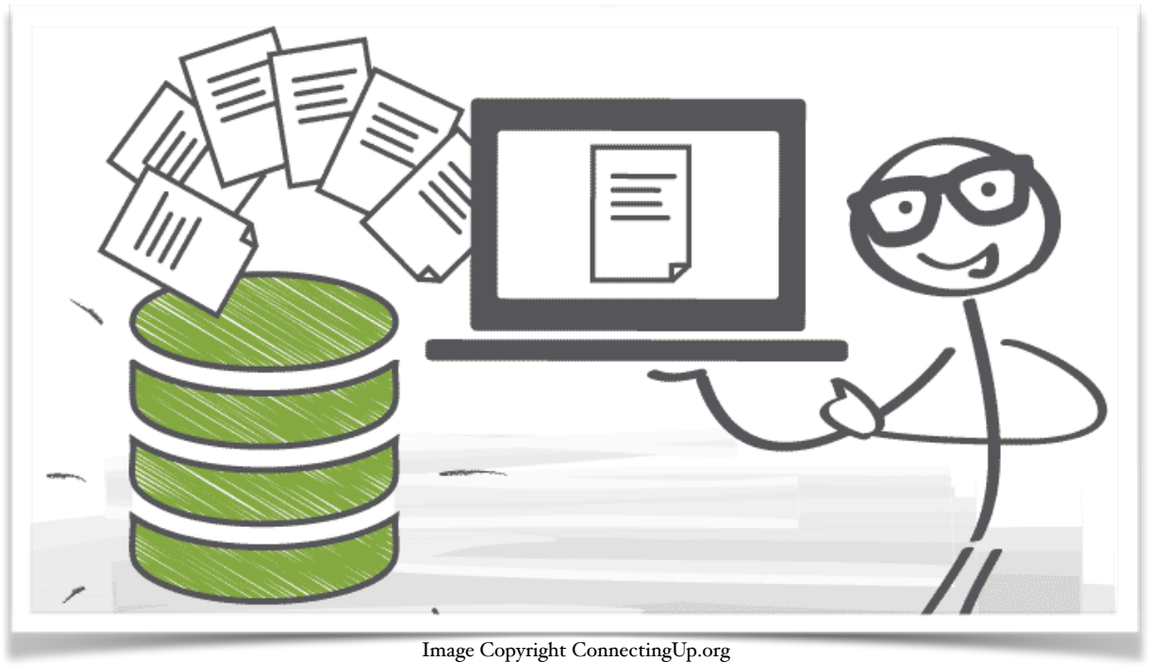


Image Copyright ConnectingUp.org

To be able to efficiently deliver marketing information and purchased products to users of our website, we will need a way to securely collect and compile their contact information. The best way for us to do this is to create a User Database.

# Features & Objectives

**Feature:** Collect customer information using web forms on our website and mobile app.

**Objective:** Use modern web security features and technology to protect the transmission of data, disclosing data-usage permissions specifically and clearly to the customer at the point of entry.

**Feature:** An internal database for storing customer information such as names, addresses, phone numbers, payment information, order history and more.

**Objective:** "Build A Wall" of security around our customers' sensitive information through government policy compliance and industry best practices to keep bad-actors out and protect them as well as our company.

# Privacy Concerns

- Government Policy Compliance
- Privacy and Security Best Practices
- Clear and Specific Policies
- Full Disclosure of How Data is Used

# Government-Mandated Requirements

- **COPPA - The Children's Online Privacy Protection Act** requires that there is special care taken for users under the age of 13, relating to keeping confidentiality and allowing parents to give or revoke consent. More info at https://www.privacypolicies.com/blog/coppa/

- **CalOPPA - The California Online Privacy Protection Act** focuses primarily on the implementation of a strong privacy policy. The requirements for which can be found at https://www.privacypolicies.com/blog/caloppa/

- **DNT (Do Not Track) - The DNT clause** is about disclosing whether we respond to users' DNT requests (a modern browser feature, learn more at https://allaboutdnt.com/).

# Government-Mandated Requirements

- **GDPR - General Data Protection Regulation** requiring us to clearly communicate what users consent to separately and descriptively. More information can be found at https://www.privacypolicies.com/blog/gdpr/

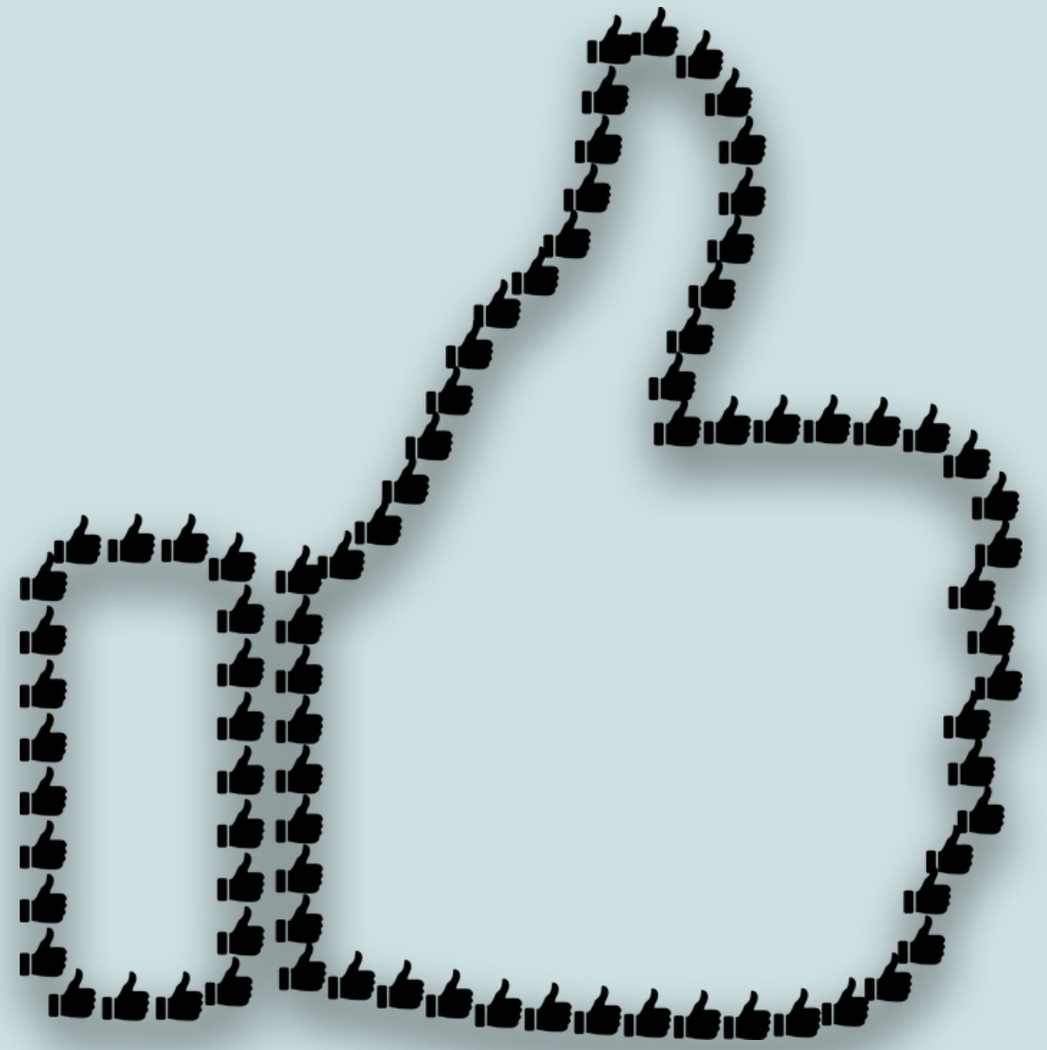
- **EU Cookies Directive (The Cookie Law)** - Requires that a disclosure is made informing users whether or not cookies are being used. More information here: https://www.privacypolicies.com/blog/eu-cookie-law/

- **PIPEDA - The Personal Information Protection and Electronic Documents Act** is Canada's main federal law relating to privacy in the private sector, requiring companies to adhere to 10 Fair Information Principles that can be read about at https://www.privacypolicies.com/blog/pipeda/

- **HIPAA - The Health Insurance Portability and Accountability Act** does not apply to us, but rather deals with health related information. More information at https://www.hhs.gov/hipaa/index.html

# Relevant Industry Best Practices and/or Recommendations

- Make data theft more difficult
- Have an elaborate password policy
- Backup data regularly
- Perform third-party security audits
- Don't store plain text passwords
- Manage employees' permissions
- Monitor network and actions
- Use at-rest encryption



Information taken from https://medium.com/tanker-blog/10-best-practices-to-protect-your-users-data-f8fb64d46f09

# Additional Thoughts

If we intend to transact business with a worldwide audience, we should consider being compliant with government policies from the EU and Canada, as well as others as they become widely adopted by the industry.